Network Camera

Software User's Manual

Table of Contents

Authentication 1
Installing the Plug-In 2
Live View 3
Configuration 6
- Camera/Video/Audio 6
  - Camera 6
  - Video 11
  - Audio 15
  - Privacy Mask Control(*) 16
- Network 17
  - IP Settings 17
  - UPnP 18
  - DDNS (dynamic domain name service) 18
  - Multicast 23
  - EasyLink™ 24
- Wireless(*) 25
  - Basic Settings 25
  - Advanced Settings 31
  - Wi-Fi Protected Setup 32
  - Event Settings 33
  - Motion Detection 38
  - Digital Input (DI)(*) 40
  - PIR(*) 41
- Notifications 42
  - FTP Settings 42
  - E-mail Settings 43
  - Samba Settings 44
  - HTTP Settings 44
  - Digital Output (DO) (*) 45
  - Audio Clip(*) 46
  - Video Clip 46
  - LED Light (*) 48
- SD Card 49
  - Storage Management (*) 49
- Maintenance 50
  - Language 50

User Management 50
IP Filter 52
Firmware Upgrade 52
Configuration 54
Reset to Default 55
Reboot 55
System 56
System Log 56
Date and Time 57
Save File Folder 58
Device Information 58

Authentication

To access the camera's live view, open a web browser and enter the IP address of the camera. A dialog window will pop requesting a username and password. As stated on the previous page, for the default username and password for the Administrator are assigned as "**admin/admin**". For accounts other than the administrator's account, the user can choose to remember the password for future convenience. It is not recommended to check this box when viewing the camera feed from a public computer.

Windows Security
The server 192.168.2.23 at NetworkCamera WGP-100-CB requires a username and password.
Warning: This server is requesting that your username and password be sent in an insecure manner (basic authentication without a secure connection).
User name
Password
Remember my credentials
OK
Cancel

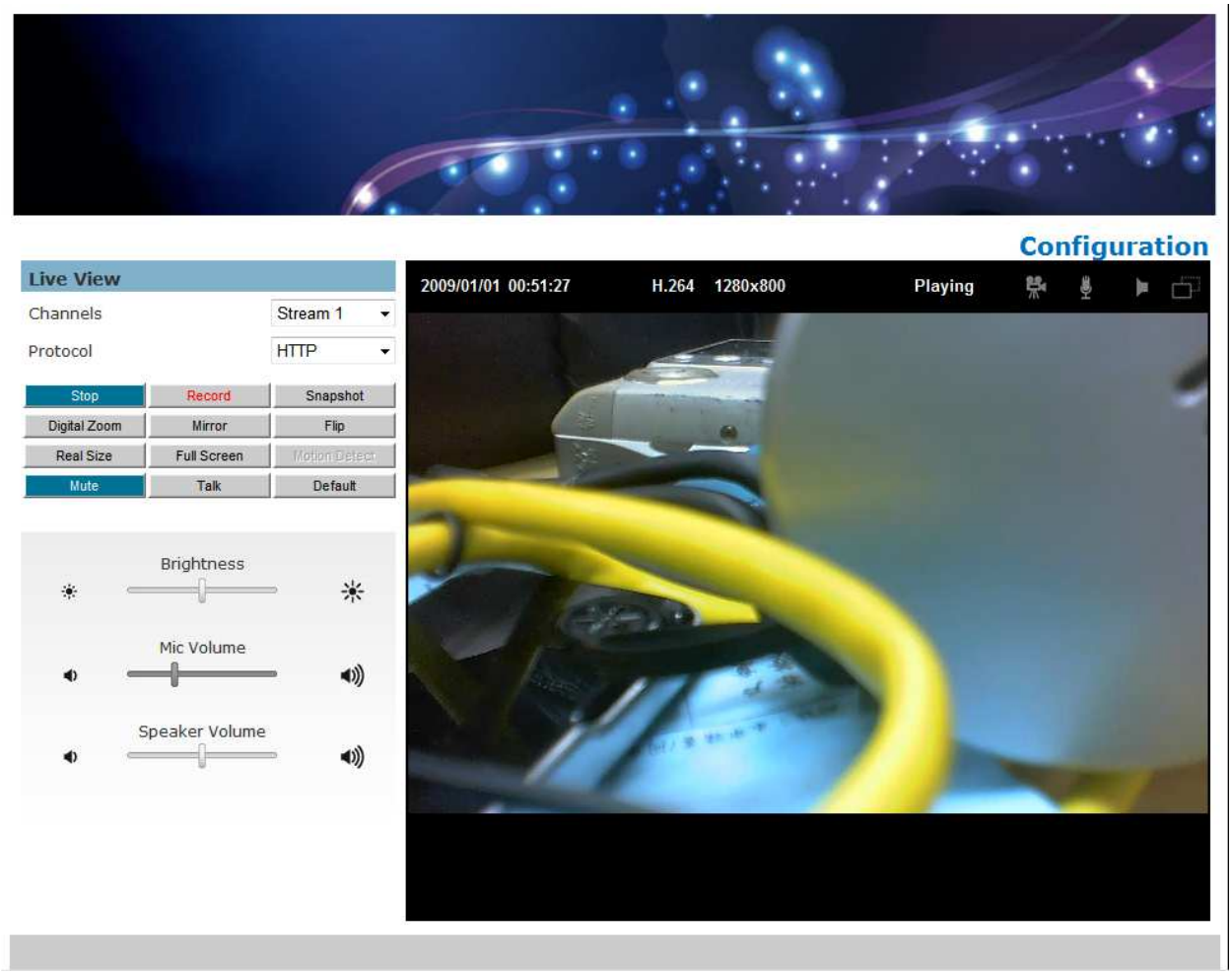
Installing the Plug-In

For the initial access to the camera in Windows, the web browser may prompt the administrator for permission to install a new plug-in for on Internet Explorer. Permission request depends on the Internet security settings of the user's PC or notebook. If the highest security level is set, the computer may prohibit any installation and execution attempt. This plug-in has been registered for certificate and is used to display the video in the browser. Click on install to proceed. If the web browser does not allow the administrator to continue the installation, check the Internet security option and lower the security levels or contact the networking supervisor or IT for help.

Internet Explorer - Security Warning
Do you want to install this software?
Name: NetworkCamera.cab
Publisher: Gemtek Technology Co., Ltd.
More options
Install
Don't Install
While files from the Internet can be useful, this file type can potentially harm your computer. Only install software from publishers you trust. What's the risk?

NOTE – If an error occurred or the plug-in fails to install, it is because the version of the Electronic Signature is newly released and the VeriSign has not been submitted to Microsoft Windows update for validation. Therefore, plug-in will not have its root certificate. If IE discovers that there is no root certificate after the user's PC connects to the camera, it will automatically redirect to VeriSign Web site to download and install the latest root certificate to make the installation successfully. If the user's computer is able to connect to camera but unable to access the internet, then the installation will fail because the computer will not be able to download the latest root certificate. This problem can be resolved if computer can be connect to the internet and the camera at the same time and will not recur when Windows update patches become available.

Live View



NOTE - (*) These are optional features. Please refer to the Product List for the full list of optional features available for the product.

Live View is the default page that opens when accessing the camera. Live video is displayed directly in the browser window.

- ***Stream1~2 Channels***

The network camera offers simultaneous several streams for optimized quality and bandwidth. Go to Configuration → Camera/Video/Audio → Video to configure the codec compression and video resolution or refer to the Video configuration page.

- ***HTTP/TCP/UDP protocol***

HTTP – This unicast method can be used to traverse firewalls. Firewalls are commonly configured to allow the HTTP protocol, thus allowing RTP to be tunneled.

TCP - This protocol guarantees the complete delivery of streaming data and provides better video quality. The downside of using this protocol is that the quality of its real-time effect is less than that of the UDP protocol.

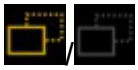
UDP - This protocol allows for more real-time audio and video streams. However, network packets may be lost due to network burst traffic and images may be broken. Activate UDP connection time-sensitive responses are more important than video quality.

LED Control(CB-series Professional only) – Use the drop-down menu to adjust the brightness of the camera's LED.

Recording on/off - Displays the status of recording video

MIC on /off - Displays the status of the MIC volume

Speaker on/off - Displays the status of the Speaker

 MD on/off - Displays the status of Motion Detection

- **Brightness -** Drag the slider bar to adjust the image brightness level.
- **Mic volume** - Drag the slider bar to adjust the microphone volume.
- **Speaker volume -** The built-in speaker will play sound from an audio clip from the computer microphone when it is enabled.
- **Play or Stop** - Play or stop the video.
- **Recording** - Record video to a computer.
- **Snapshot** - Capture and save still images.

- **Digital Zoom** - Enable the digital zoom operation.
- **Mirror** - Horizontally reflect the display of the live video.
- **Flip** - Vertically reflect the display of the live video.
- **Real Size** - View the object in real size. Press it again to switch back to normal mode.
- **Full Screen** - Switch to full screen mode. Press the “Esc” key to return to normal mode.
- **Motion Detection** - Enable the motion detection alert function.
- **Mute** – Turn off the sound.
- **Talk(*)** – To communicate through the camera using the computer MIC.
- **Set Default** – Reset to default settings.

NOTE

1. The <Camera Control Panel> functions have no effect on the recorded video. Whatever changes are made to the <Camera Control Panel> **will not** be applied to the recorded video.

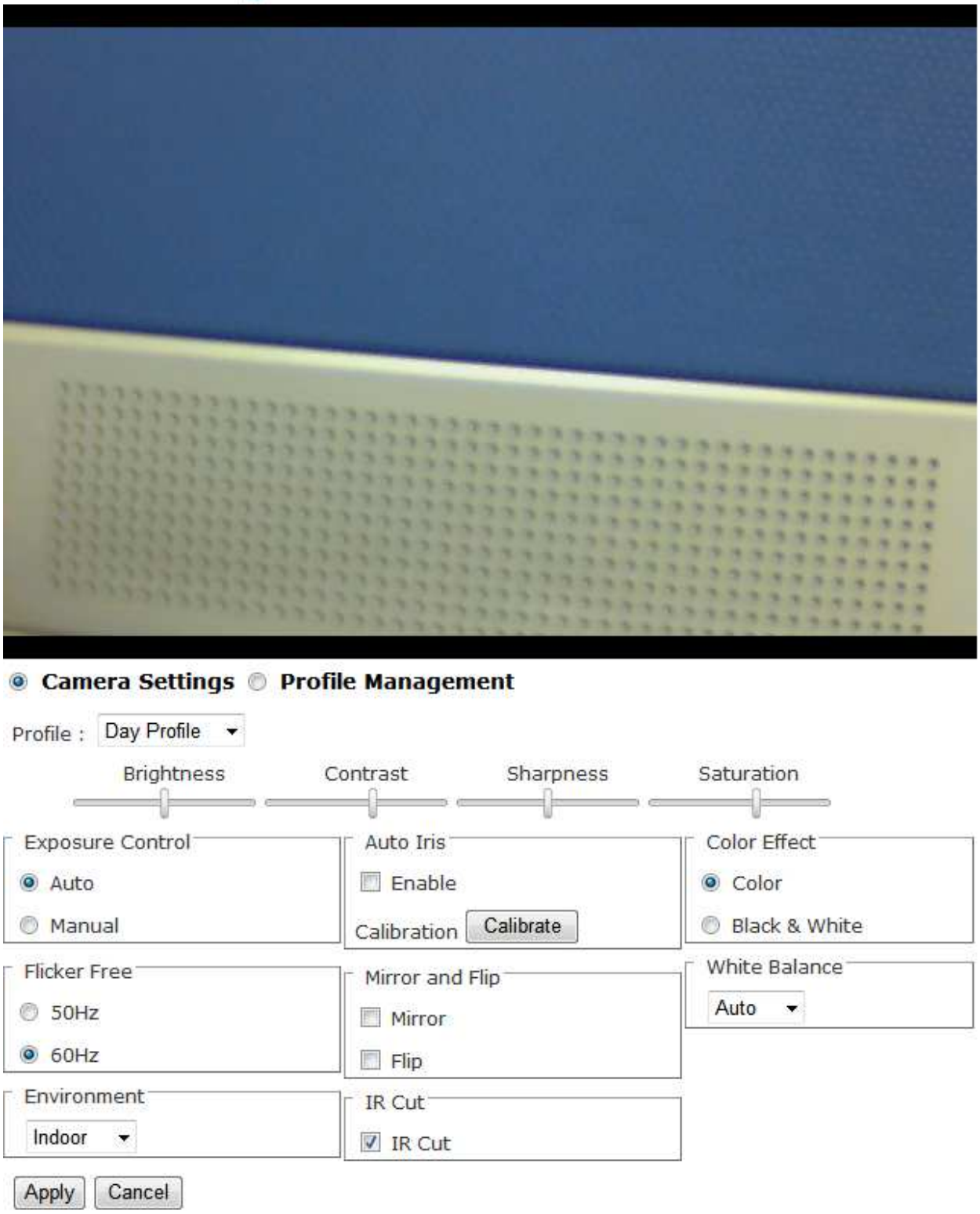
Configuration

Click <**Configuration**> on the main page to change the camera settings pages.

NOTE - Only Administrators can access the Configuration page.

Camera/Video/Audio

Camera



Profile – Up to five profiles can be created for different lighting environments. Day and night are default profiles and users can create up to three additional profiles. Select a profile from the drop-down menu or select different icons to change profile settings.

Brightness - Drag the bar to adjust the image brightness level from -5 to +5.

Contrast - Drag the bar to adjust the image contrast level from -5 to +5.

Sharpness - Drag the bar to adjust the image sharpness level from -5 to +5.

Saturation - Drag the bar to adjust the image saturation level from -5 to +5.

Exposure Control

Auto: The camera will automatically control exposure.

Manual: Select this option to define the exposure manually

Flicker-Free – Eliminates the problem of flicker.

Mirror and Flip

Mirror - Enable to horizontally reflect the display of the live video.

Flip - Enable to vertically reflect the display of the live video.

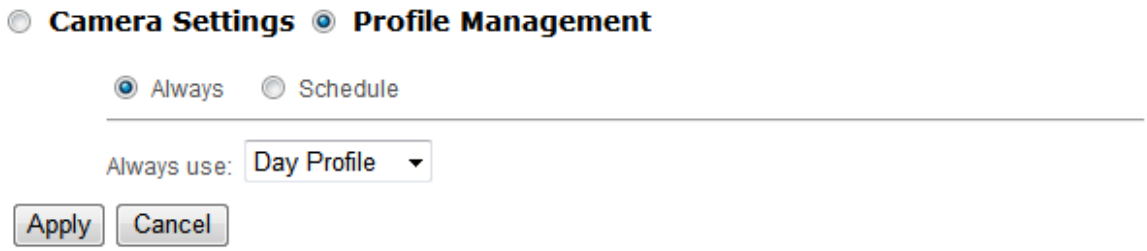
Environment –Select outdoor or indoor mode based on the conditions.

IR Cut (*) (Only available with models with a IR Cut) **–** Deactivate or activate the IR cut filter

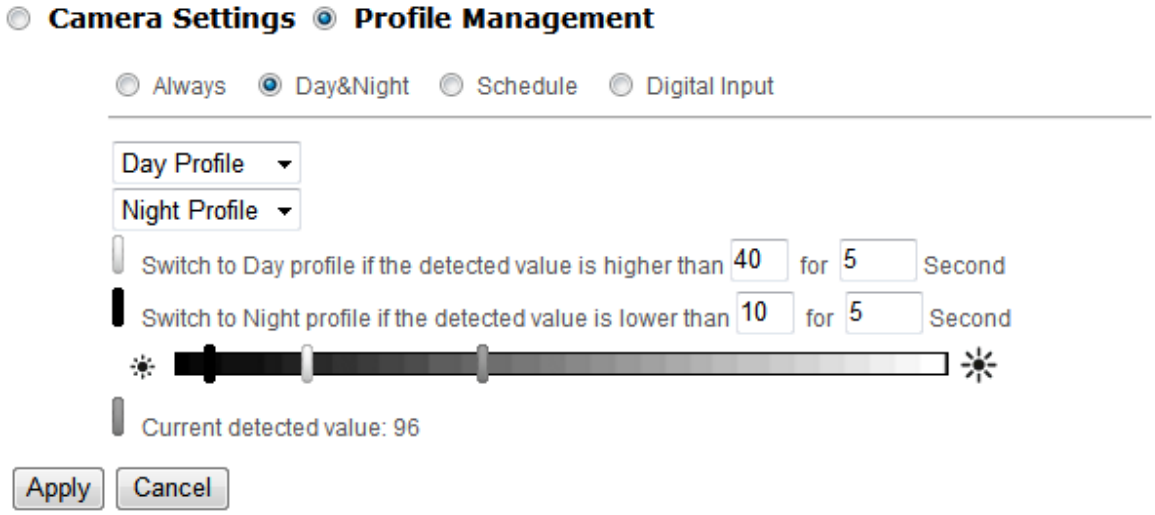
Color Effect - Select to display color or black and white video streams.

White Balance - White balance is a camera setting that adjusts for lighting in order to make Black & white.

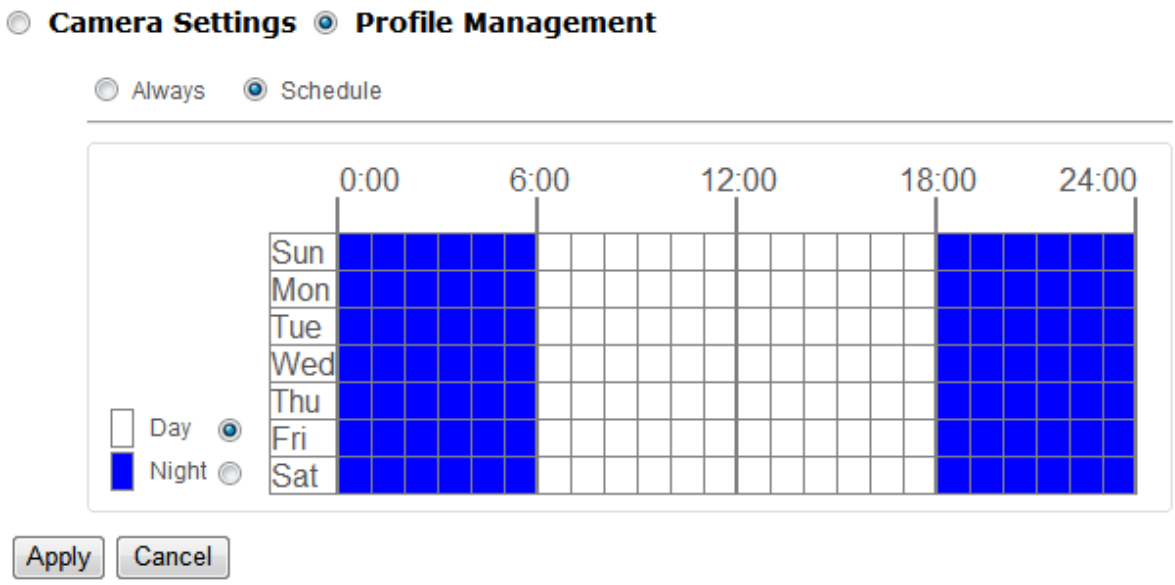
Profile Management: Profiles can be scheduled to change at scheduled times or under different lightening changes.



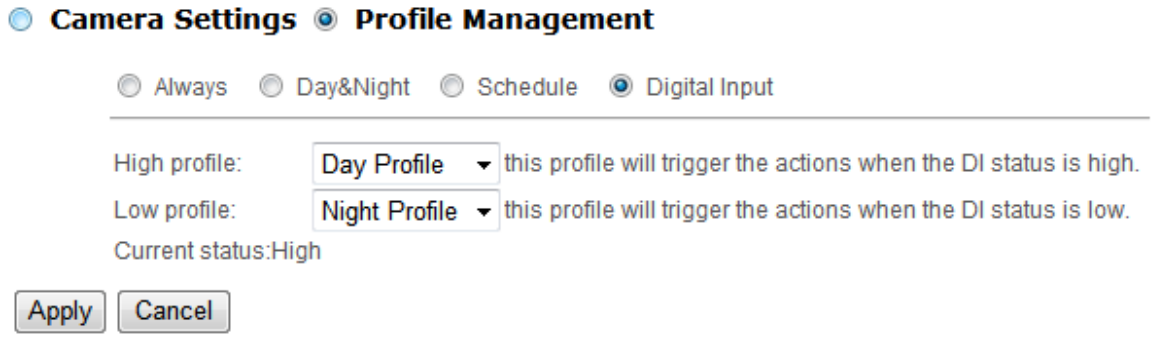
Always- Select Always to use a single profile. Select the profile from the drop down menu.



Day & Night (*) (Only available with models with a light sensor Mode) - Select Day & Night to schedule two profiles for day and night. Select profiles from the drop down menu for the Day and Night Profiles.



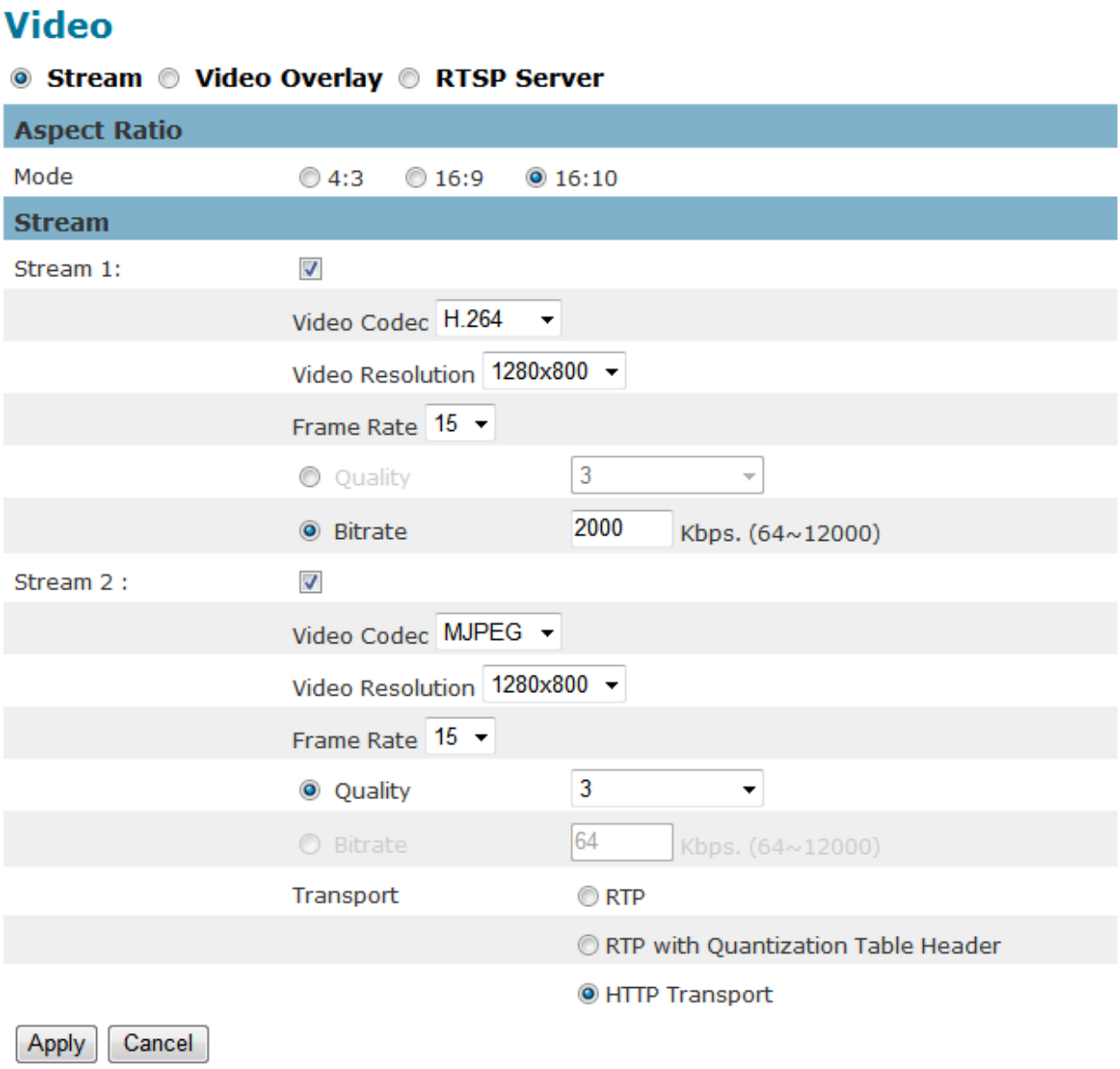
Schedule – Select Schedule to schedule specific time periods for different profiles.



Digital Inputs (*) (Only available with models with a DI terminal) - Select Digital Input to have the profile management controlled by an external sensor. Select profiles from the drop down menu. Profiles will change according to different trigger voltage levels. Click **Apply** to apply settings or **Cancel** to cancel changes.

Video

The Network Camera offers several separate streams for different viewing options.



Stream 1 ~2

Aspect Ratio – Select the width to height image aspect ratio.

Video Codec - The Network Camera offers three choices of video codec standards for real-time viewing: H.264, MPEG-4 and MJPEG.

Video Resolution - Select from the drop-down menu to choose the best resolution recording settings.

Frame Rate - Select the frame rate from drop-down menu. When selecting from

Video Codec option, the frame rate ranges from 1 to 30 fps. Set a higher frame rate for smoother video quality.

Video quality and bit rate - Choose either “quality” or “bitrate” to control the video quality with video codec at H.264 or MPEG4. Only “quality” can be chosen when video codec at MJPEG is selected. Set the bitrate higher for a better video quality.

Transport-

RTP: The Real-time Transport Protocol (RTP) defines a standardized packet format for delivering audio and video over IP networks.

RTP with Quantization Table Header : Choose this option to explicitly include JPEG quantization table in the RTP stream [RFC 2435, section 3.1.8].

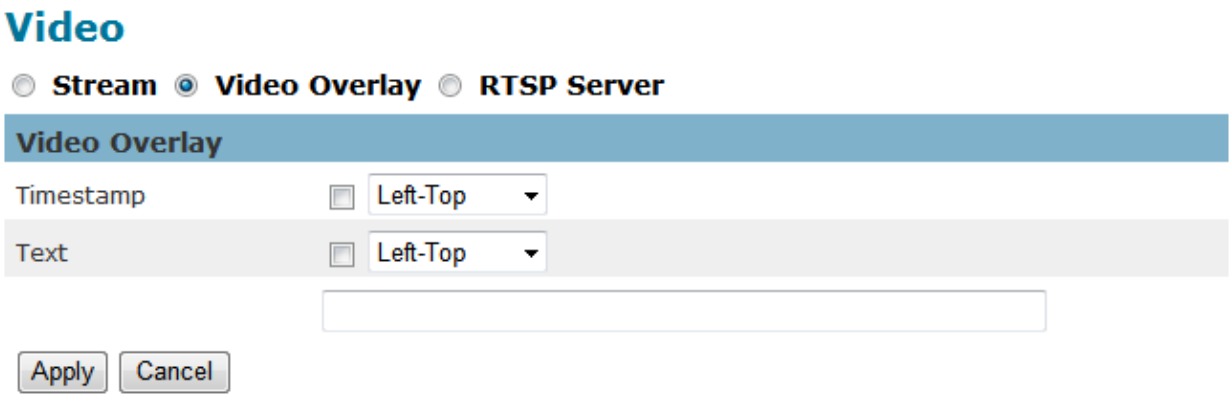
HTTP Transport : If MJPEG is used for Video Codec, HTTP Transport protocol must be enabled to remotely access the video stream.

NOTE - a higher bitrates will use higher network bandwidth. The video quality can be set between Level 1 to Level 6, with Level 6 producing the best image quality.

NOTE – HTTP Transport is for non-IE browser used only.

Click **Apply** to apply settings or **Cancel** to cancel changes.

Video Overlay



Timestamp

To display the date and time on the screen during live view, check “Enable” to enable the timestamp function and select the display position from the drop-down menu.

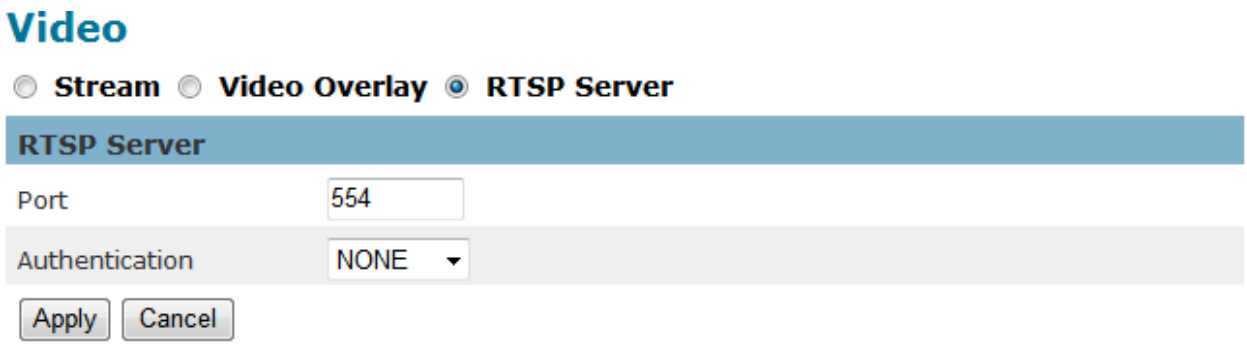
Text

To make a note about the camera, check “Enable” and select the display position from the drop-down menu. Enter a video description in the text box.

Click **Apply** to apply settings or **Cancel** to cancel changes.

NOTE - The video overlay will only take effect in stream 1.

RTSP Server



To utilize RTSP authentication, the user must first set a password for the camera.

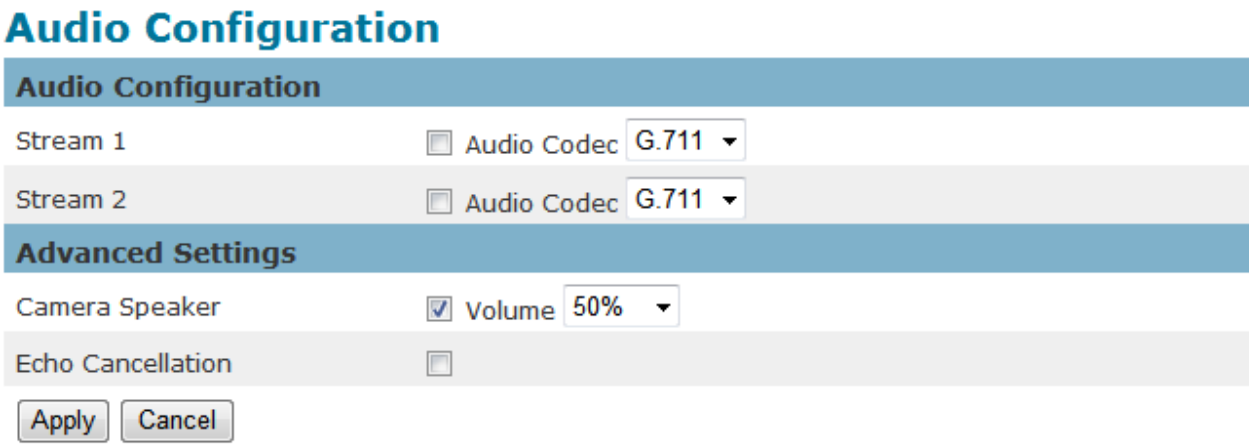
RTSP (Real-Time Streaming Protocol) controls the delivery of streaming media. By default the port number is set to 554.

Authentication - Depending on the network security requirements, the camera provides two types of security settings for streaming via RTSP protocol: NONE and DIGEST.

If DIGEST authentication is selected, user credentials are encrypted using MD5 algorithm, thus providing better protection against unauthorized access.

Audio

The administrator can set up several streams for the camera for different viewing devices. The administrator can enable or disable the audio function on either stream. If audio enable is selected, select the Audio codec from the drop-down menu.



Advanced Settings

Camera MIC - The Network Camera supports two-way audio communication so that operators can transmit and receive audio simultaneously. By using the Network Camera's built-in microphone and an external speaker, users can communicate with people who are within range of the Network Camera.

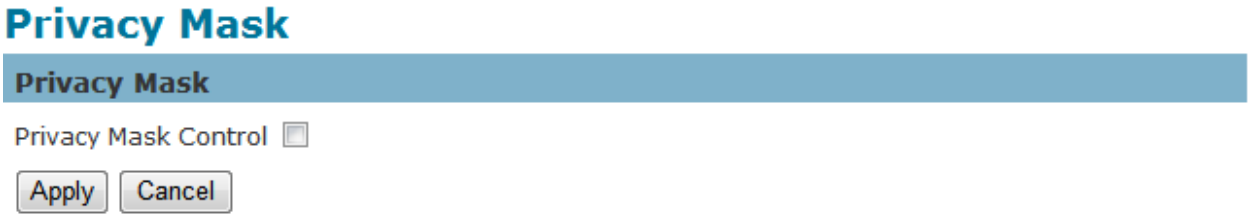
Camera Speaker – If the speaker is enabled, select the volume from the drop-down menu.

Echo Cancellation Enabled - Enable to avoid an echo.

Click **Apply** to apply settings or **Cancel** to cancel changes.

Privacy Mask Control(*)

The Cube camera is equipped with a privacy feature which allows users to mask the camera's live view. A black screen will be displayed in place of the live view window. This application is particularly useful when the camera is being used for home surveillance. With the privacy button, the user can have privacy while they are going about their daily life.



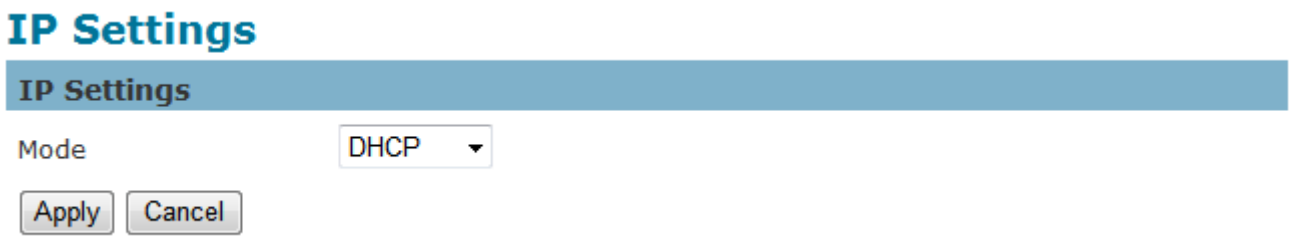
Privacy Mask Control – Enable the Privacy Mask control to remotely mask the camera's live view.

Click **Apply** to apply settings or **Cancel** to cancel changes.

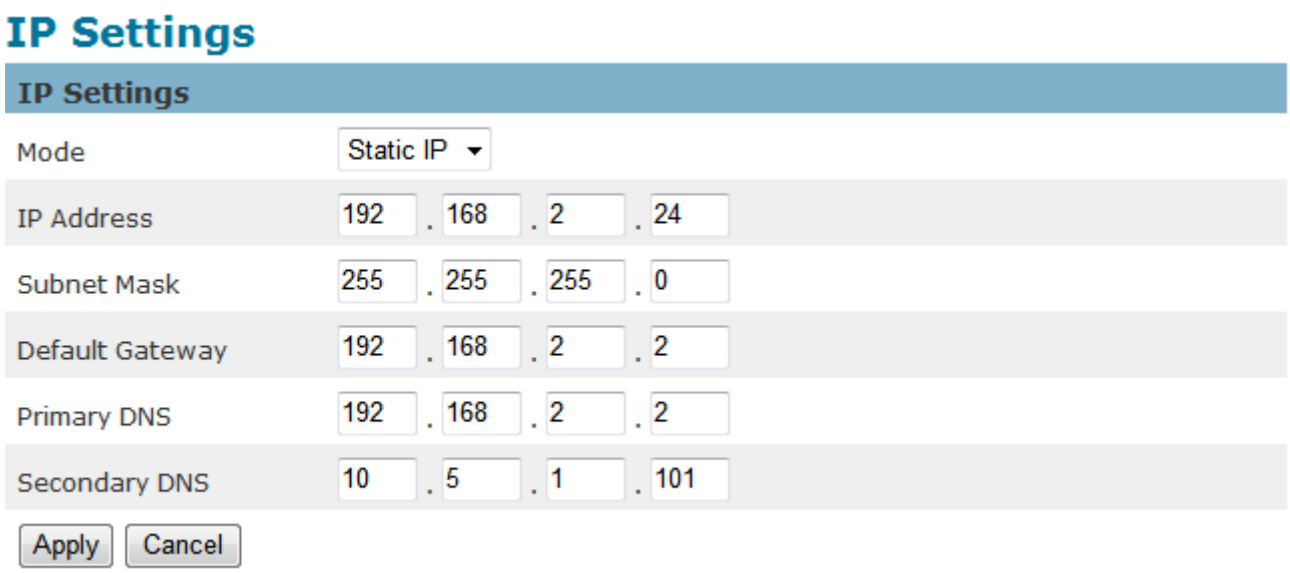
Network

IP Settings

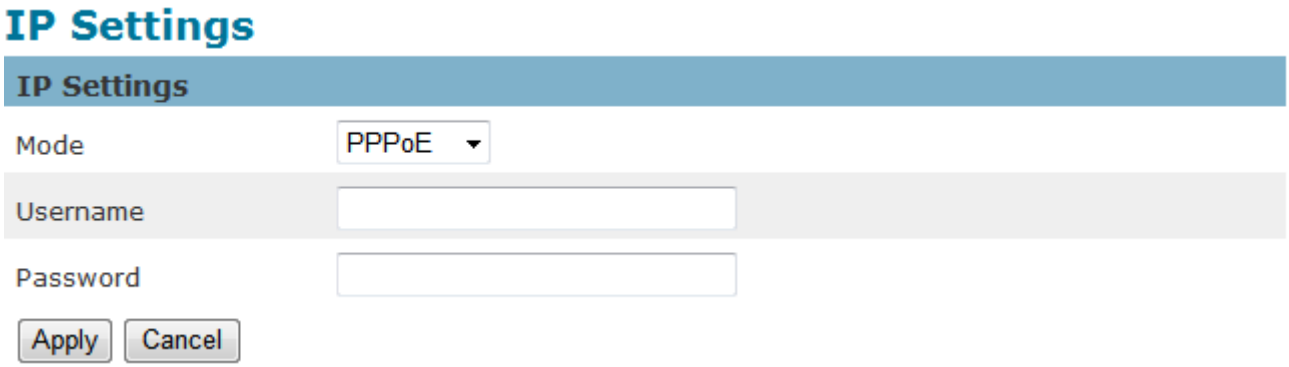
This section explains how to configure a wired network connection for the camera. There are several ways to setup the camera over the Internet: (1) obtain an available dynamic IP address assigned by a DHCP server, (2) use a static IP, or use PPPoE (Point-to-point over Ethernet). Select the desire setup mode from the IP settings drop-down menu.



1. **DHCP –**If this option is selected, the camera will automatically obtain an available dynamic IP address from the DHCP server each time it connects to the LAN.



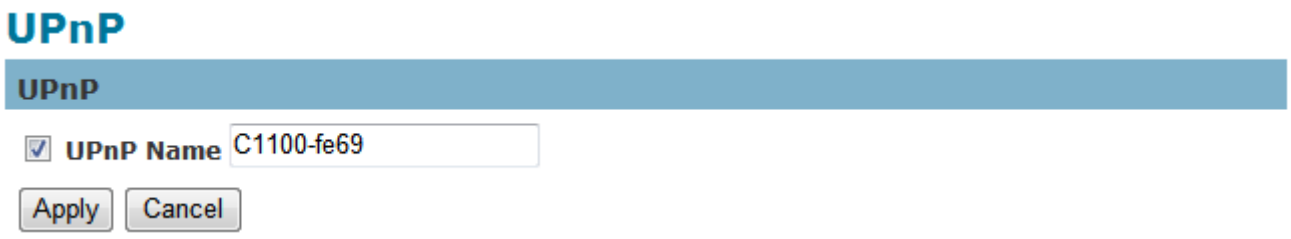
2. **Static IP -** Select this option to manually assign a static IP address to the camera. Enter the static IP address, Subnet mask, Default Gateway, Primary and Secondary DNS provided by the ISP.



3. **PPPoE** (Point-to-point over Ethernet)**:** Use this mode if connecting to the Internet through a DSL Line. **NOTE** - To utilize this feature, it requires an account provided by an Internet Service Provider. Enter the user name and password provided by the ISP. Click **Apply** to apply settings or **Cancel** to cancel changes.

UPnP

Universal Plug and Play (UPnP) simplifies the process of adding a camera to a local area network. Once connected to a LAN, the camera will automatically appear on the intranet. Click “Enable” to enable this function and enter an UPnP name which the camera will appear under on the intranet.

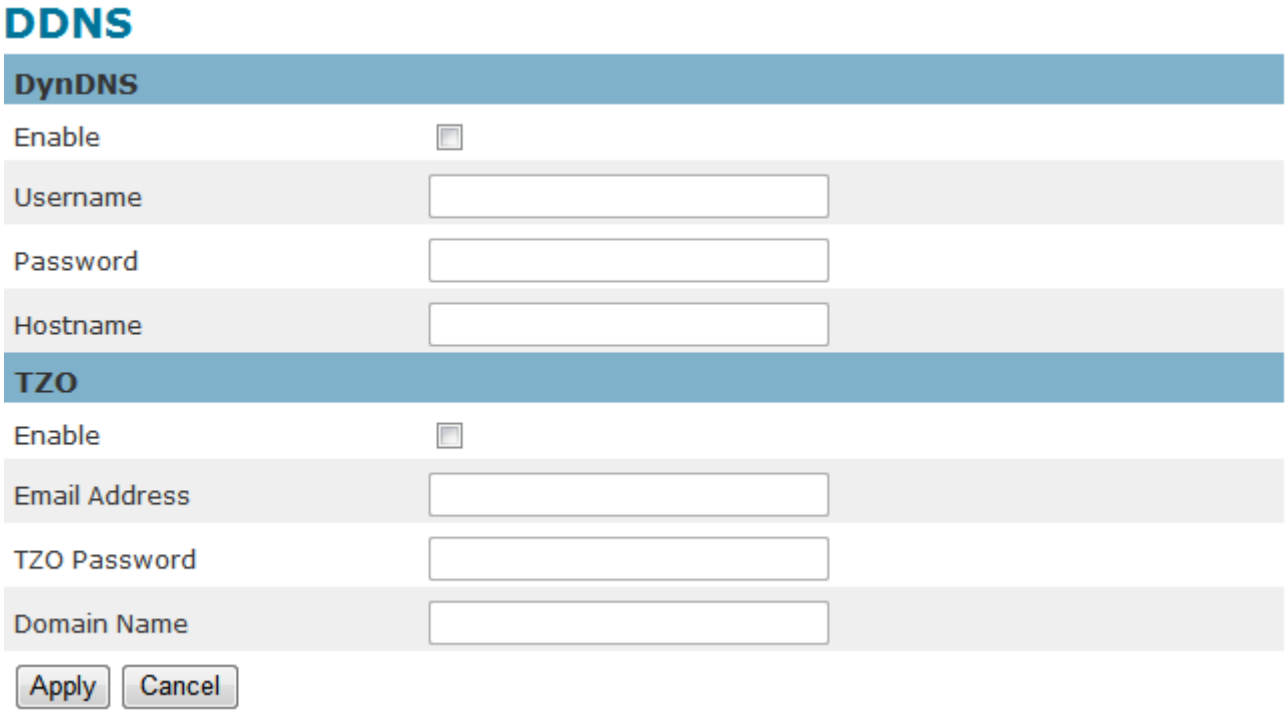


Click **Apply** to apply settings or **Cancel** to cancel changes.

DDNS (dynamic domain name service)

DDNS links a domain name to an IP address, allowing users to easily access their camera even with a changing IP address. Network cameras are compatible with three DDNS service

providers (1) DynDNSand (2) TZO **NOTE** - Before utilizing this function; please apply for a dynamic domain account from a DDNS provider.



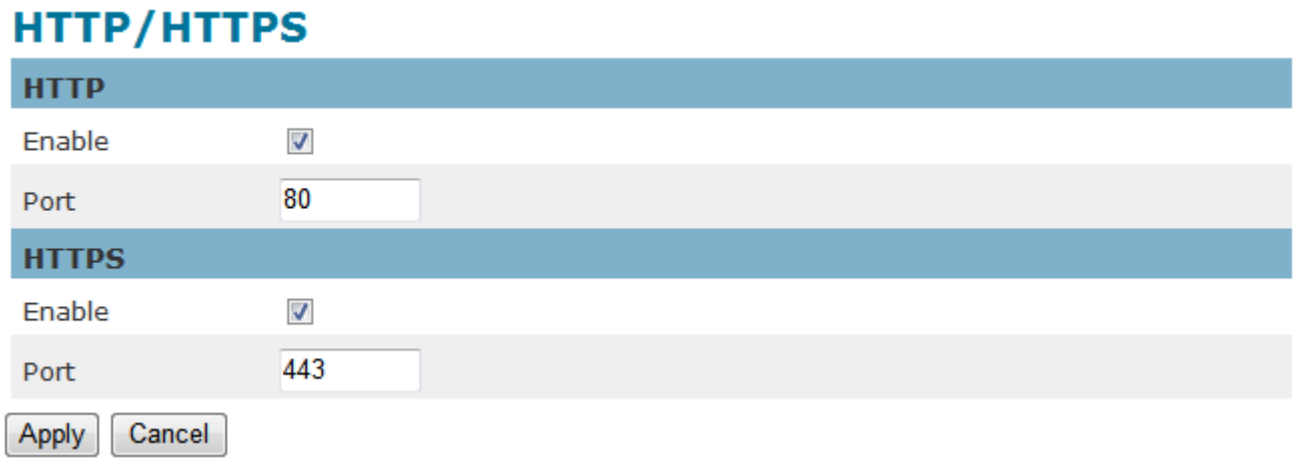
DynDNS – Enable the DynDNS to allow the camera to have a fixed host and domain name. Refer to the DynDNS website (www.dyndns.com) to apply for a dynamic domain account. When an account has been created, enter the username, password and hostname.

TZO

TZO is a DDNS provider which allows users to create a dynamic DNS. Refer to the TZO website (http://www.tzo.com/) to apply for a dynamic domain account. When an account has been created, enter the e-mail address, password and domain name.

Click **Apply** to apply settings or **Cancel** to cancel changes.

HTTP/HTTPS



HTTP – (Hypertext Transfer Protocol) - This protocol allows for TCP protocol quality without having to open specific ports for streaming. Users inside a firewall can utilize this protocol to allow streaming data through.

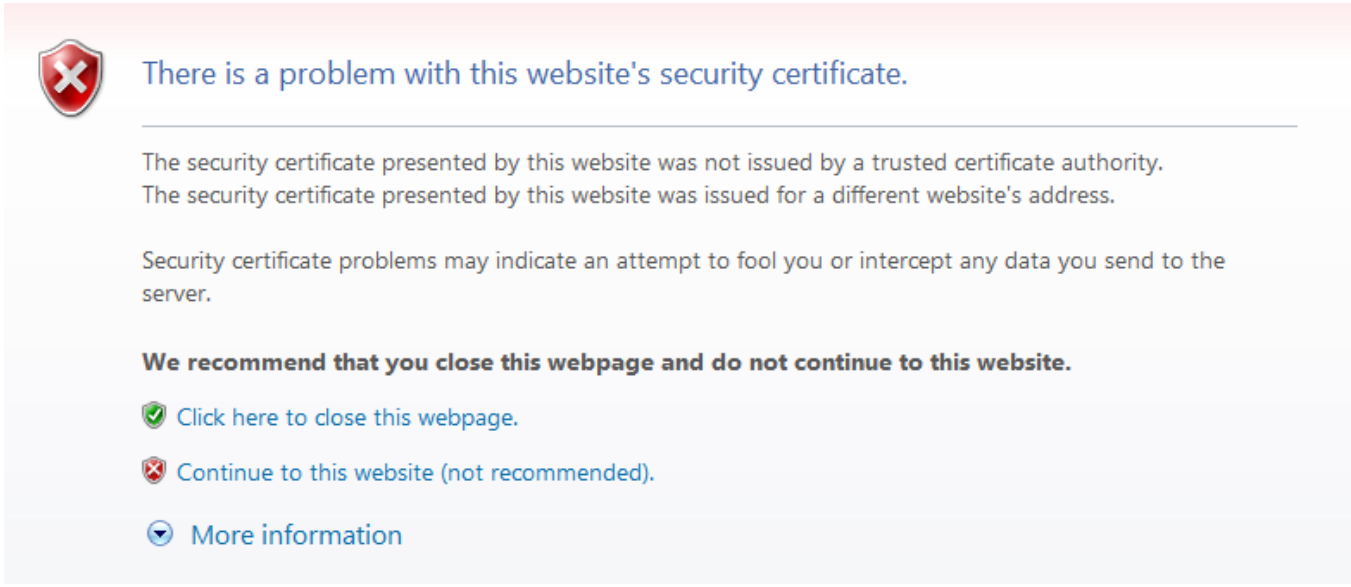
HTTPS - (Hypertext Transfer Protocol over SSL) - This protocol allows authentication and encrypted communication over SSL (Secure Socket Layer). It helps protect streaming data transmission over the Internet on a higher security level than HTTP.

Click “Enable” to enable and **Apply** to apply settings or **Cancel** to cancel changes.

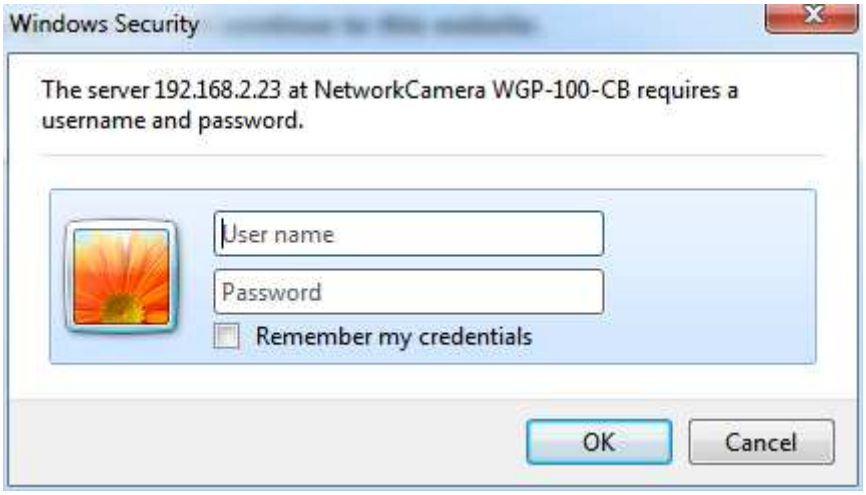
.

To enable HTTPS, users have to create and install a certificate.

1. Click “Continue to this website” to install.

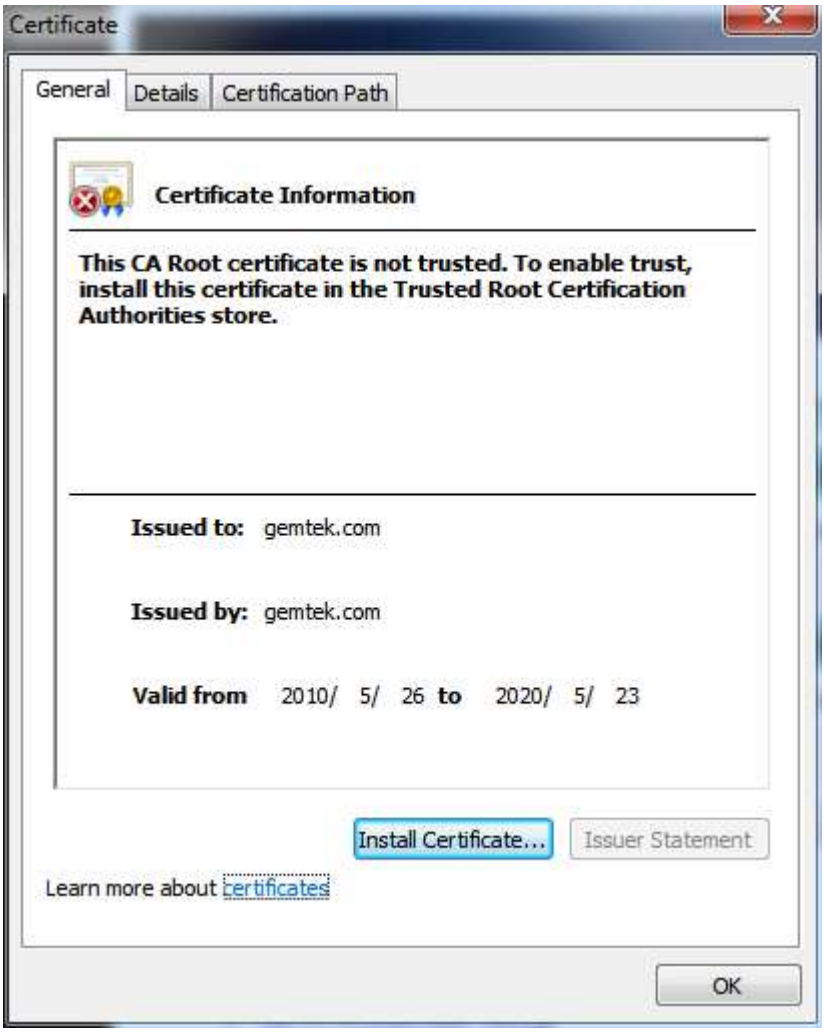

There is a problem with this website's security certificate.
The security certificate presented by this website was not issued by a trusted certificate authority.
The security certificate presented by this website was issued for a different website's address.
Security certificate problems may indicate an attempt to fool you or intercept any data you send to the server.
We recommend that you close this webpage and do not continue to this website.
Click here to close this webpage.
Continue to this website (not recommended).
More information

2. Enter the User name and Password of the camera.

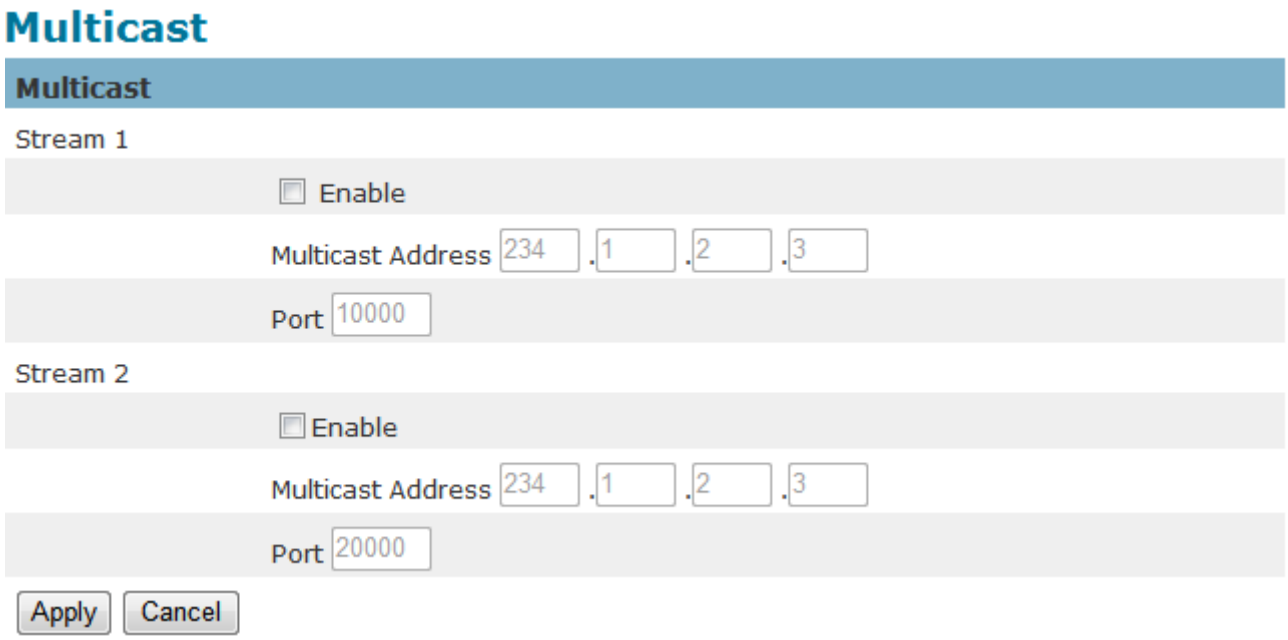


3. Click “Certificate Error” on the top right corner of the window to view the certificate.

4. Click “Install Certificate” and follow the steps to finish the installation.


Certificate
General
Details
Certification Path
Certificate Information
This CA Root certificate is not trusted. To enable trust, install this certificate in the Trusted Root Certification Authorities store.
Issued to: gemtek.com
Issued by: gemtek.com
Valid from 2010/ 5/ 26 to 2020/ 5/ 23
Install Certificate...
Issuer Statement
Learn more about certificates
OK

Multicast



Multicast sends a video stream to the multicast group address and allows multiple clients to acquire the stream at the same time by requesting a copy from the multicast group address. Therefore, multicast can effectively save Internet bandwidth. The RTSP (Real-Time Streaming Protocol) controls the delivery of streaming media.

Click “Enable” to enable Multicast stream 1 or Multicast stream 2. The default value for multicast address and port are 234.1.2.3 and 10000. Use different port number for different streams. It is recommended to use the default values.

NOTE - Using the IP address of the Network Camera enables access to the video.

Example: rtsp://192.168.1.1/channel1

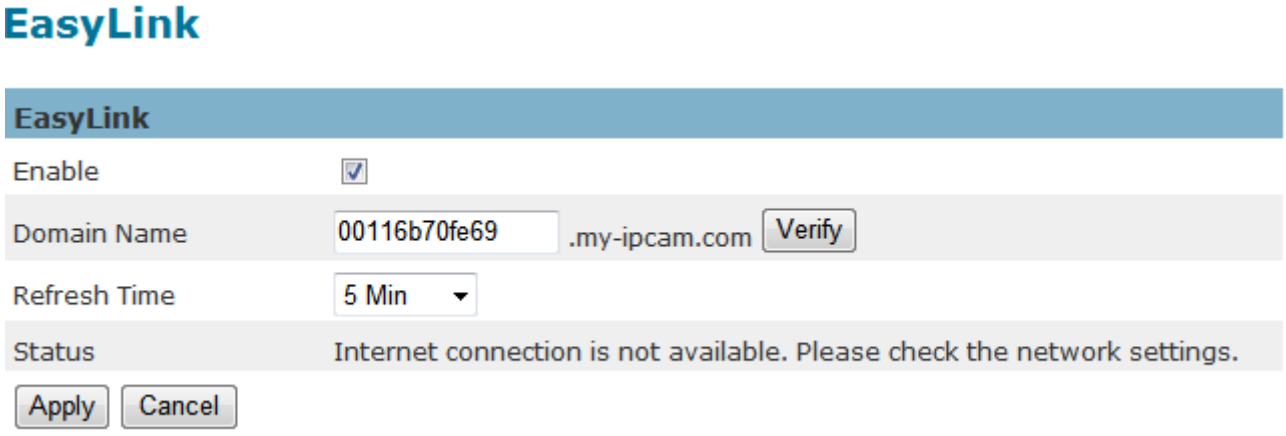
Click **Apply** to apply settings or **Cancel** to cancel changes.

EasyLink™

EasyLink™ is a unique function which allows users to assign a unique EasyLink name to their network camera's IP address. There is no need to configure the router to open up ports or remember hard-to-memorize IP addresses. When this function is enabled, users can log onto [uniqueEasyLinkname].my-ipcam.com to view the camera's web GUI and live view.

1. Check the box to enable EasyLink™.
2. If Auto mode is selected, the following page will be displayed.

   NOTE - This mode is recommended.
3. Enter a unique EasyLink name whose length must be between 5-32 characters. Verify that the EasyLink name is available.



NOTE - The EasyLink function will not work if the following conditions occur:

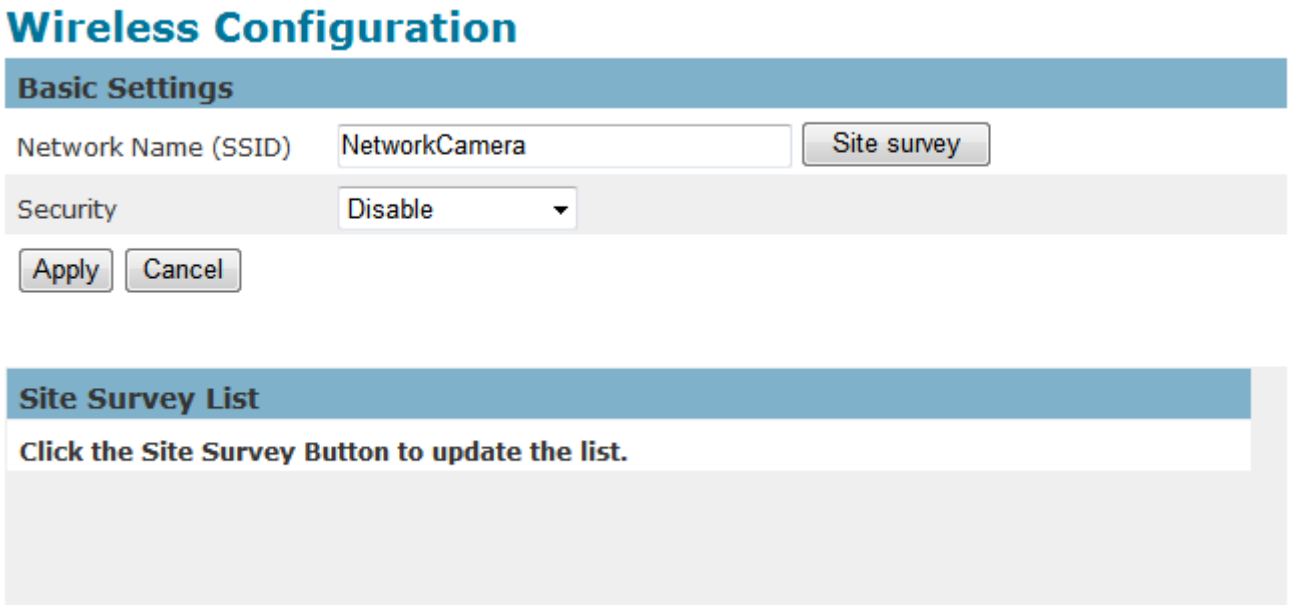
1. The camera cannot be located behind a double NAT network.
2. The camera's IP address cannot be assigned to specific port numbers using the router's port forwarding.
3. EasyLink uses UPnP to exchange port information with the router. The camera must connect to the internet through a router which supports UPnP.

Wireless(*)

These settings control how a Network Camera interacts with a wireless network. Users can identify the wireless network and enable wireless encryption.

NOTE – This function is only available for Wireless models.

Basic Settings



Network Name (SSID) - The Service Set Identifier (SSID) is the network name used to identify the wireless signal emitted from a wireless camera. It is case-sensitive and can be up to 32 characters long.

Wireless devices have a default SSID set by the factory. Wireless products use **NetworkCamera** as the default name. It is recommended for users to rename their SSID to something unique in order to distinguish their wireless device from surrounding wireless networks.

NOTE - Be careful when including personal information when naming the SSID as it is viewable by anyone browsing for wireless networks.

Security - Encryption protects data transmitted over a wireless network. Wi-Fi Protected Access (WPA-Personal/WPA2-personal) and Wired Equivalent Privacy (WEP) offer different levels of security for wireless communication. A network encrypted with WPA-Personal/WPA2-personal is more secure than a network encrypted with WEP because WPA-Personal/WPA2-personal uses dynamic key encryption. To protect the information as it passes through the airwaves, it is recommended to enable the highest level of encryption supported by the network equipment.

Site Survey – Survey the local area for available wireless networks. The user should select their Local Area Network (LAN) from the Site Survey List.

Wireless Configuration

Basic Settings

Network Name (SSID) NetworkCamera Site survey

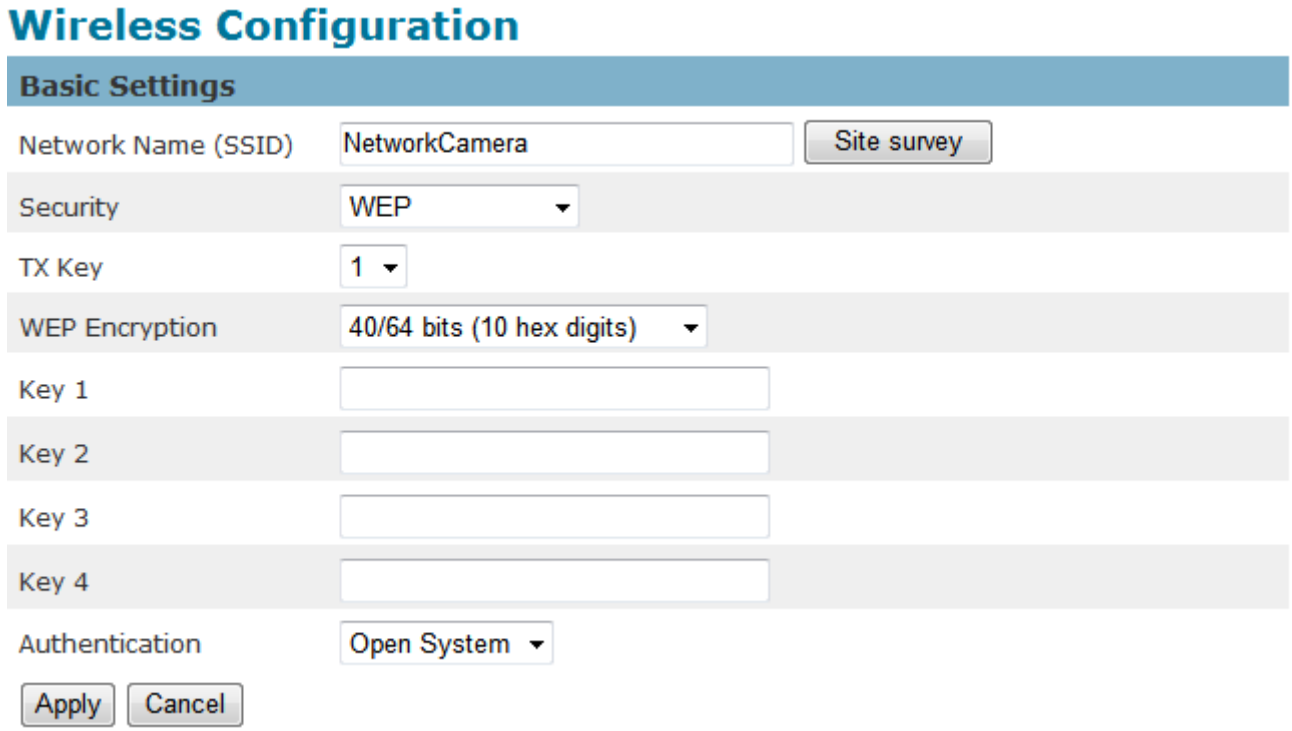
Security Disable

Apply Cancel

Site Survey List

Network Name (SSID)	Mode	Security	Channel	Signal	Select
Brickcom_B	11b/g/n	WEP	1	57%	Select
Test_Cavin	11b/g/n	WPAPSK/AES	1	42%	Select
dennis-Brickcom	11b/g/n	NONE	1	68%	Select
Test_Blue	11b/g/n	NONE	1	23%	Select
belkin.44c8	11b/g/n	NONE	1	52%	Select
jj-test	11b/g/n	WPA2PSK/AES	1	47%	Select
WhiteLable_Arvin	11b/g/n	WEP	1	57%	Select
test-jacky-13ch	11b/g/n	WPAPSK/TKIP	1	63%	Select
tony_router	11b/g	WPAPSK/TKIP	2	23%	Select
blue_test_2.4g	11b/g/n	WPAPSK/AES	3	23%	Select
Test_2.4G	11b/g/n	NONE	3	2%	Select
Test_SQA	11b/g/n	NONE	3	7%	Select
BaBaHouse-I	11b/g	WPAPSK/TKIP	3	31%	Select
Brickcom	11b/g/n	NONE	6	23%	Select

WEP- Wired Equivalent Privacy (WEP) is a basic encryption method which transmits network broadcast messages using radio signals. It is not as secure as WPA.



Tx Key - Select a key from the drop-down menu.

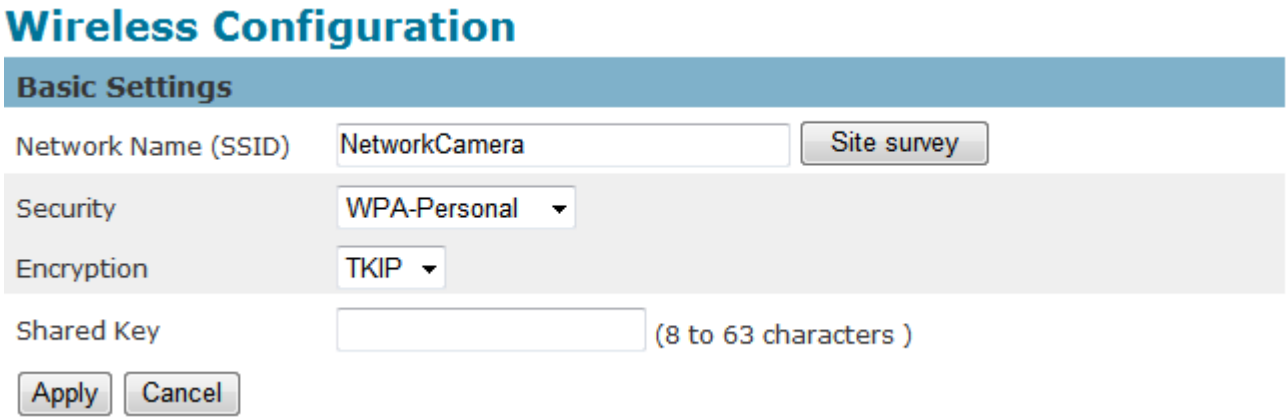
WEP Encryption - Select a level of WEP encryption: 64 bits 10 hex digits or 128 bits 26 hex digits. The default is 64 bits 10 hex digits.

Key 1-4 - Enter the WEP key(s) manually.

Authentication - The default is set to Open System, which allows either Shared Key or Auto authentication to be used. With Shared Key authentication, the sender and recipient use a WEP key for authentication. With Auto authentication, the sender and the recipient do not use a WEP key for authentication.

Click **Apply** to apply settings or **Cancel** to cancel changes.

WPA-Personal - WiFi Protected Access (WPA)-Personal

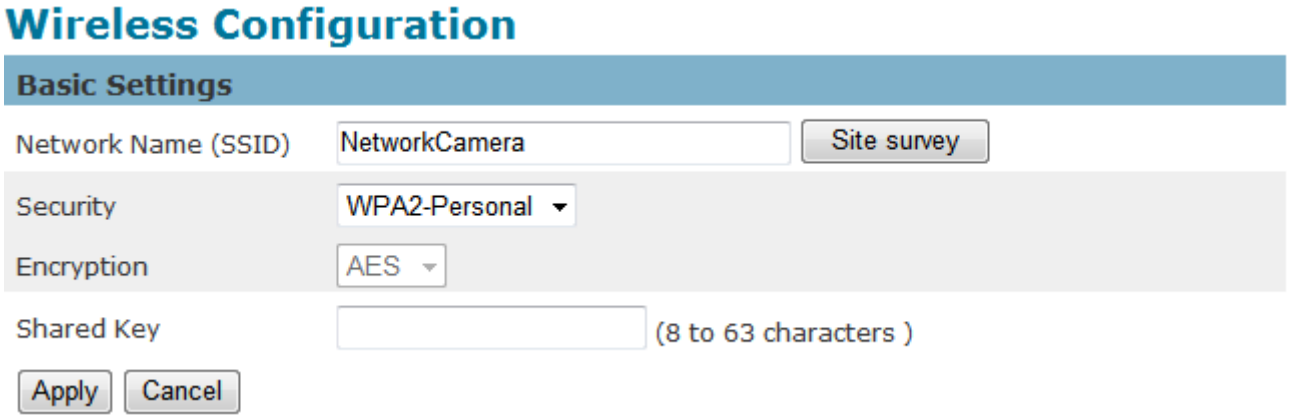


Encryption - Supports two encryption methods with dynamic encryption keys: Temporal Key Integrity Protocol (TKIP) and Advanced Encryption Standard (AES). Select the algorithm type from the drop down menu: TKIP or AES. The default is TKIP.

Shared Key - Enter the key shared between the Router and the server keys. Enter a password of 8-63 characters.

Click **Apply** to apply settings or **Cancel** to cancel changes.

WPA2-Persona l - WiFi Protected Access (WPA2-Personal)

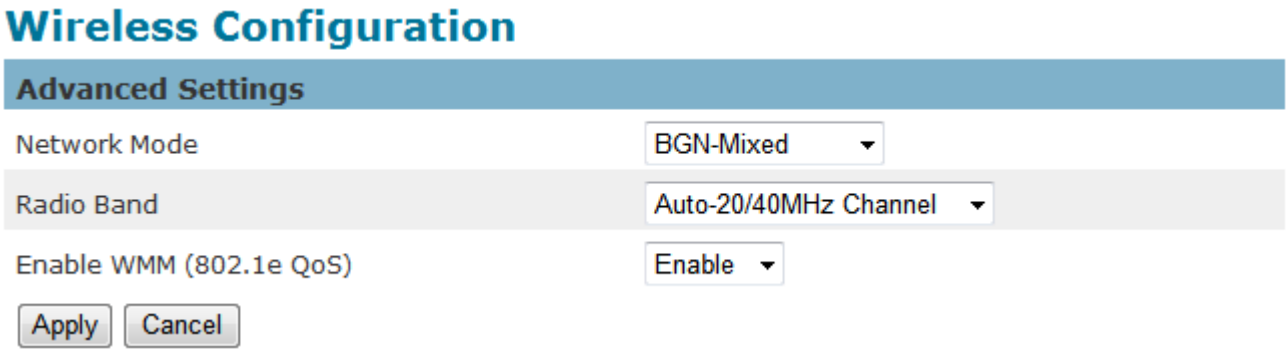


Encryption - WPA2 supports AES encryption method with dynamic encryption keys.

Shared Key - Enter the key shared between the Router and the server keys. Enter a password of 8-63 characters.

NOTE - If using WPA or WPA2, each device in the wireless network must use the same WPA or WPA2 method and shared key or else the network will not function properly.

Advanced Settings



Network Mode - From the drop-down menu, select the wireless standards running on the network.

- If there are Wireless-B, Wireless-G and Wireless-N (2.4GHz) devices on the network, use the default setting, **BGN-Mixed**.
- If there are Wireless-B and Wireless-G devices on the network, select **BG-Mixed**.
- If there are only Wireless-B devices on the network, select **Wireless-B Only**.
- If there are only Wireless-G devices on the network, select **Wireless-G Only**.
- If there are only Wireless-N (2.4GHz) devices on the network, select **Wireless-N Only**.

Radio Band - The settings are available for the Auto-20/40MHz channel and Standard-20 MHz channel.

Enable WMM (802.1e QoS) - WMM is a wireless Quality of Service feature that improves quality for audio, video, and voice applications by prioritizing wireless traffic. To use this feature, the wireless client devices on the network must support Wireless WMM. The default setting is **Enabled.** To disable this feature, select **Disable**.

Click **Apply** to apply settings or **Cancel** to cancel changes

Wi-Fi Protected Setup

Use this method if the client device has a Wi-Fi Protected Setup PIN number.

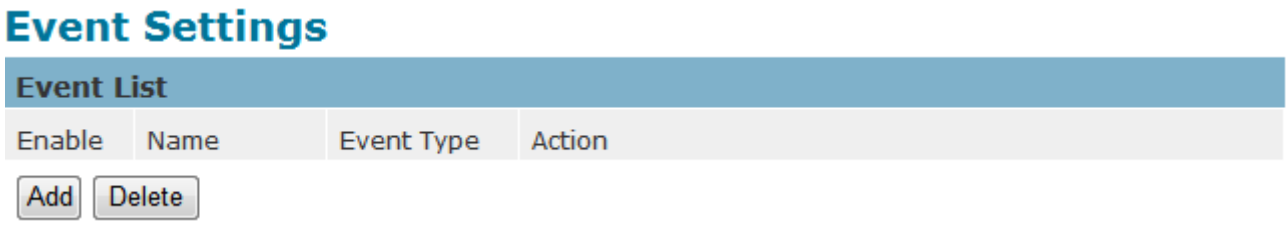
1. Enter the network name from the device in the field.
2. Click <Register> to start WPS.
3. Click “Enable” to enable the WPS Button. If this feature is not enabled, the user will not be able to use the WPS button

Click **Apply** to apply settings or **Cancel** to cancel changes.

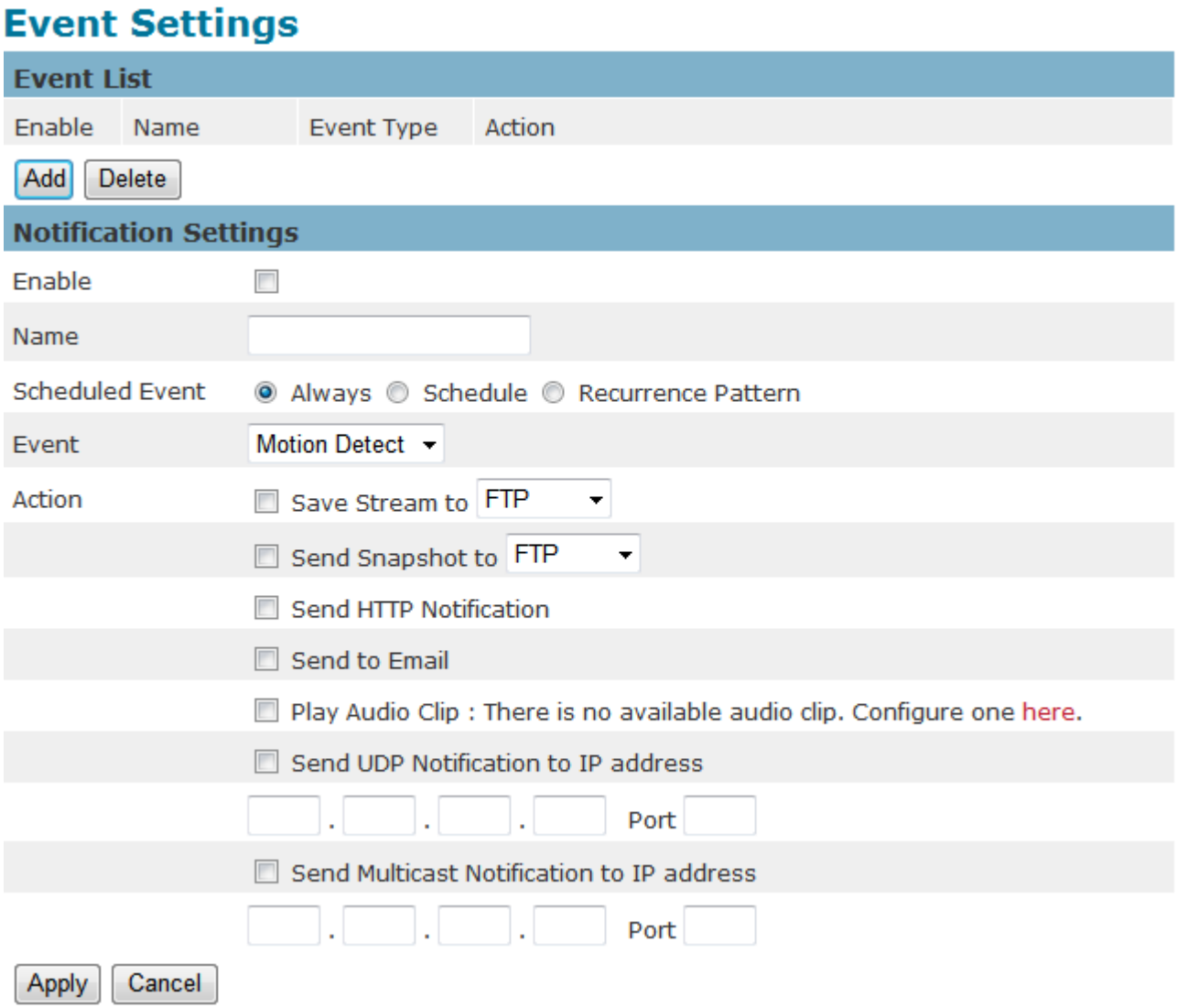
Event

Event Settings

When an event (such as unauthorized movement) occurs, the camera can be scheduled to perform certain actions. An Event Type is a set of parameters that defines these actions. This section describes how to configure the camera to perform certain actions when events occur.



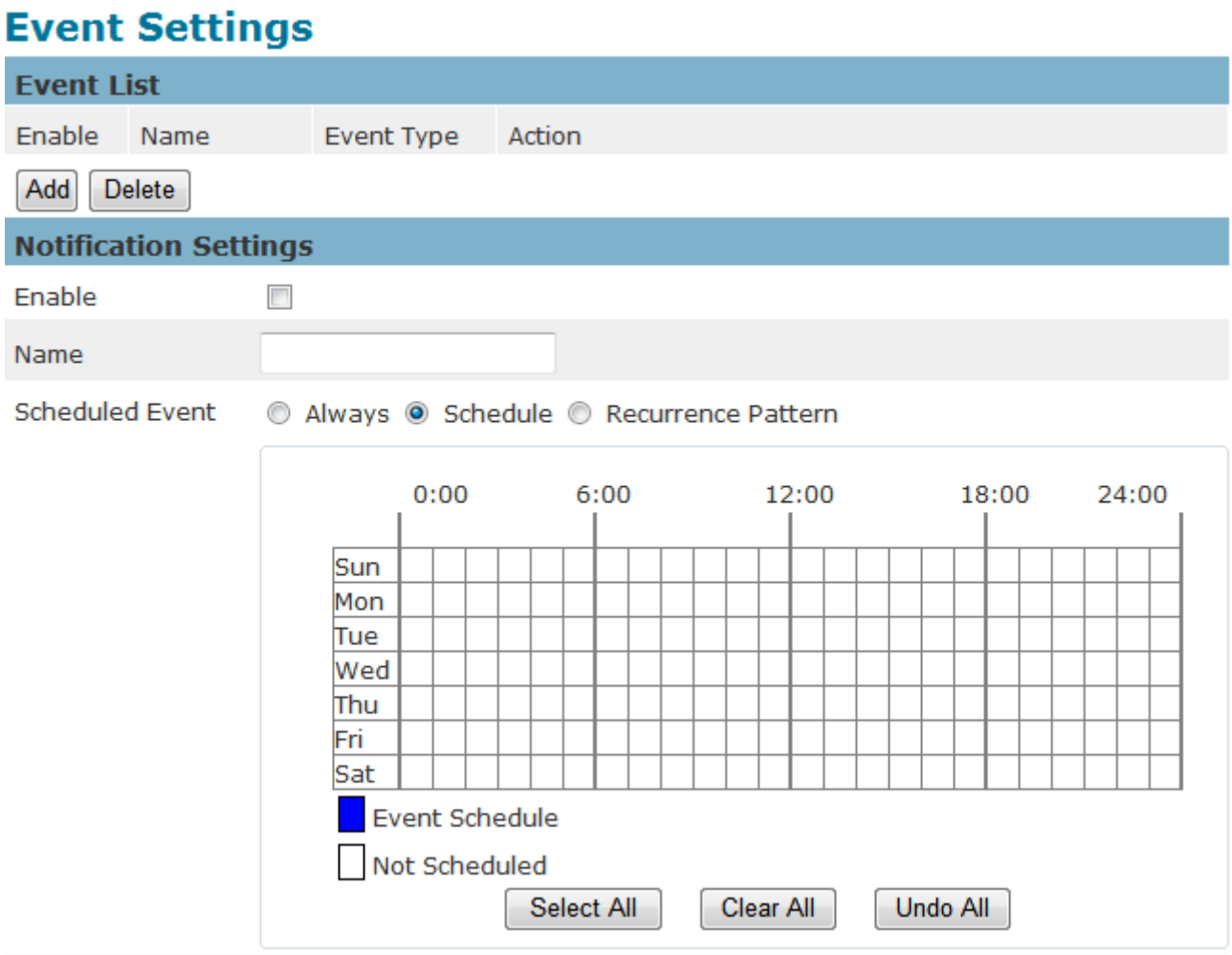
Click <Add Event> on the Event Settings page. The Event Setup page will appear.



How to Set Up an Event Schedule

Event Schedule describes how and when the camera performs certain actions.

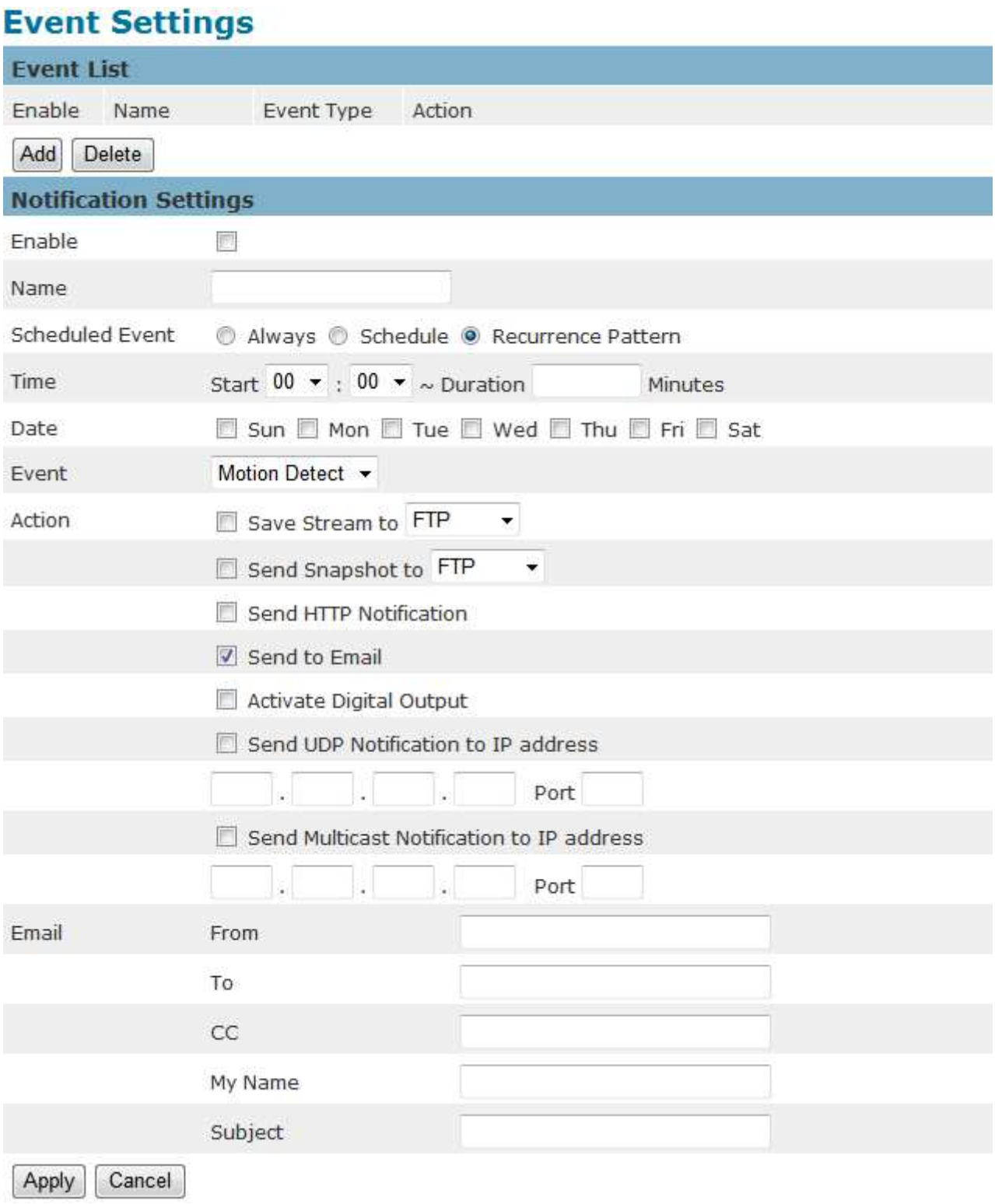
1. Check “Enable” and enter a descriptive name for the event schedule.
2. Set Event Schedule to define when the event is activated by selecting from Always (24 hours), Schedule or Recurrence pattern.
    a. If Schedule is selected from the Event Schedule, the following page will be displayed:



i. A Scheduled Event can be programmed for certain times and day.

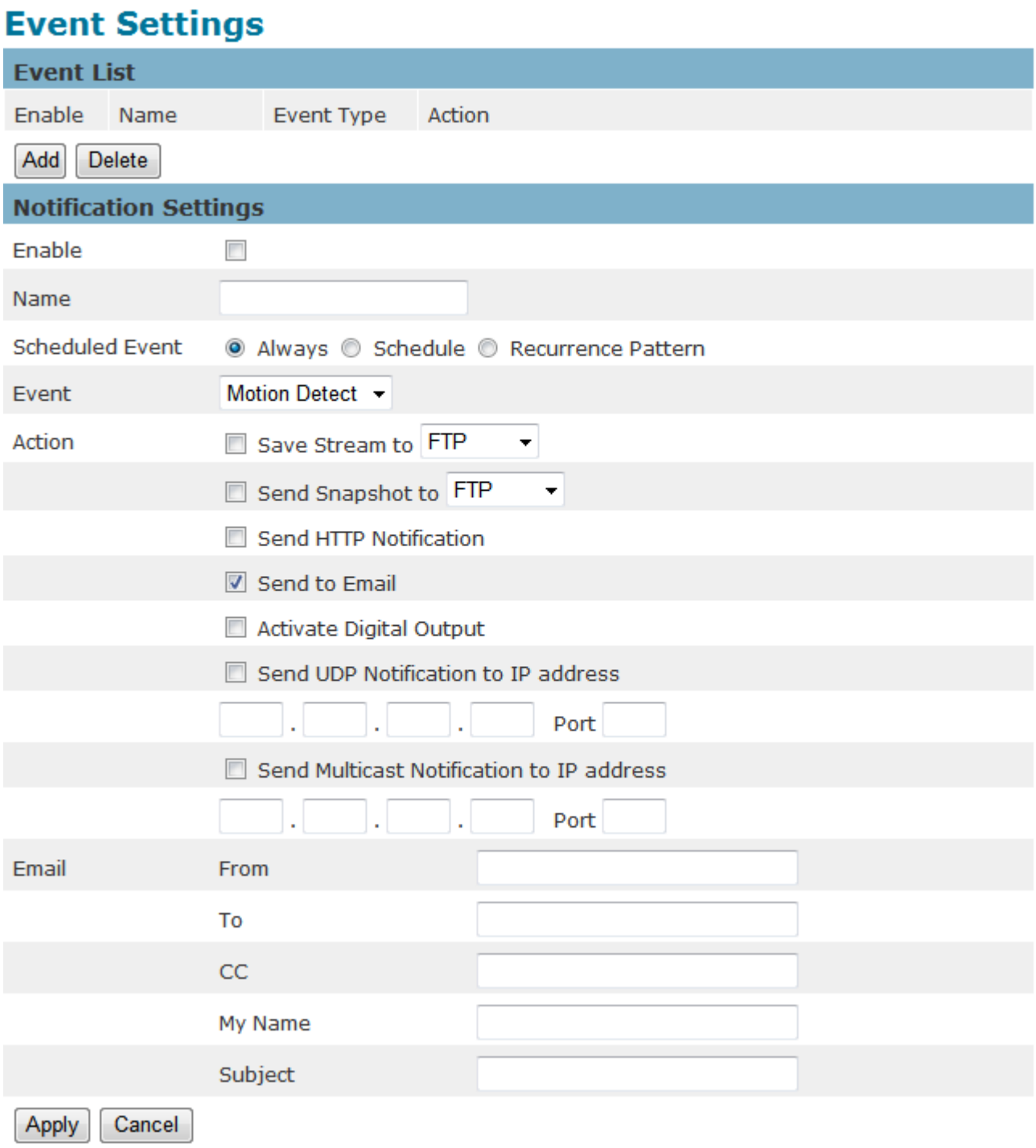
ii. Click individual boxes to schedule specific times for the camera to detect events.

b. If Recurrence Pattern is selected, the following page will be displayed.



i. An event schedule can be programmed to recur at different times according to the user's needs. Select the days for the event schedule to occur. Select a start time and specify the duration.

3. Define what will trigger an event to occur by selecting an option from the Event drop-down list.
4. Select the Actions that will occur when the event is triggered.
    a. When <Send to Email> is selected, the following page will be shown:



ii. Sender - Enter the email address of the sender.

iii. Recipient - Enter the email address of the recipient. To enter multiple recipients, separate each using a comma.

iv. Sender's Name – Enter the sender's name that will appear in the recipient's inbox.

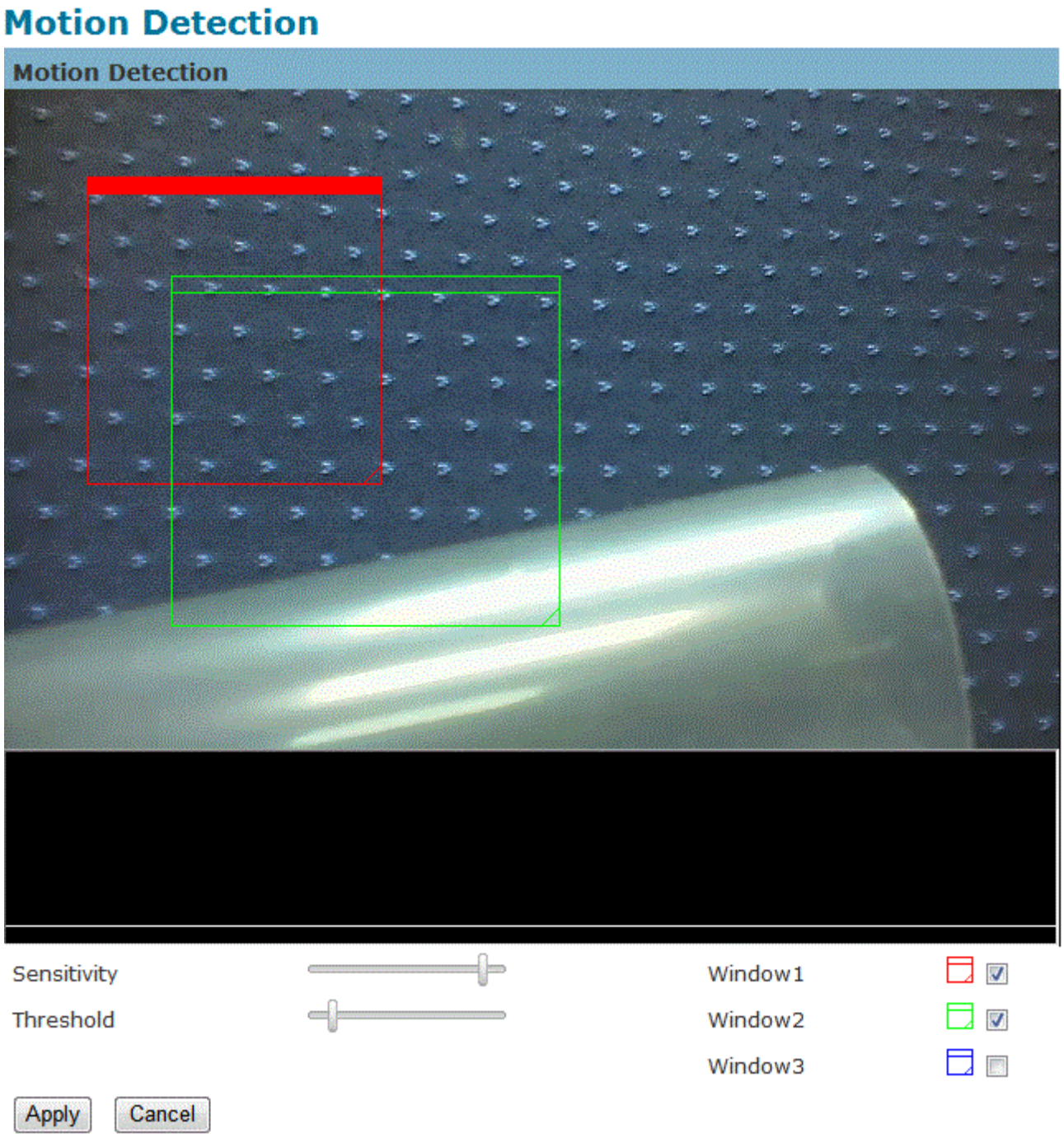
v. Subject - Enter the title of the email.

5. When complete, click **Apply** to save new event or **Cancel** to delete the event. The new event will appear on the event list.
6. To edit an event setting; select the event from the list. To remove an event setting from the list, select an event name from the list and then click <Delete Event>. Click <Add Event> to add more events.

NOTE - Refer to the Audio Clip section for more details about the "Play Audio Clip" action.

Motion Detection

Motion can be detected by measuring changes in the speed or vector of an object or objects in the monitored area. This section explains how to configure the Network Camera to enable motion detection.



Detection Setting – Use this setting to enable and define the motion detection windows. The user can defined up to three areas on the live view window for motion detection.

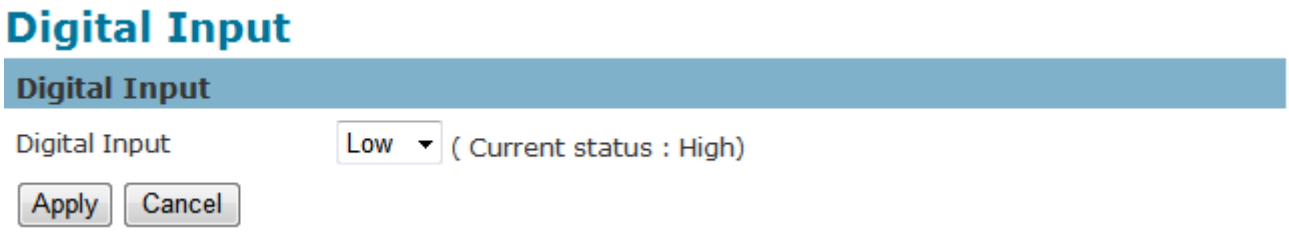
1. Select <Window1>, <Window2>, or <Window3> to adjust the motion detection window.
2. Check the box to enable the window.
3. Use the mouse to resize or move the motion detection window.
4. Adjust the “Sensitivity” level. Lower sensitivity levels will result in more activity needed

to trigger an event.

5. Adjust the “Threshold” to change the threshold level. The higher the threshold, the larger objects need to be to trigger an event.
6. The chart below the Live View window indicates the activity level of the Motion Detection window. When motion is detected by the camera and exceeds the defined threshold, a red bar will appear. Users can use this feature as a trigger source to send photos or videos to a remote server via email or FTP.

   Click **Apply** to apply settings or **Cancel** to cancel changes.

Digital Input (DI)(*)



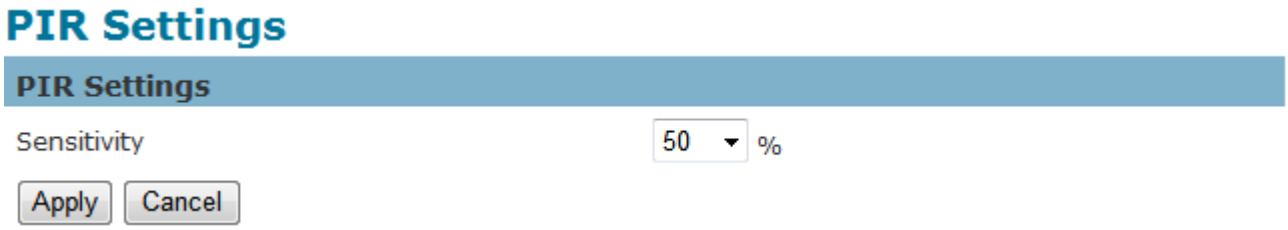
The DI socket allows the IP camera to receive input from an external device.

The external device should have the ability to drive voltage on the connected DI wire to the triggering voltage level in order to notify the IP camera of any event of interest. The IP camera will then process the event notification according to the specific event rules.

Triggering voltage Level: LOW, HIGH, Rising and Falling

Users should select the option according to the capability of their external device.

PIR(*)



The PIR (Passive InfraRed) sensor measures infrared light radiating from objects in its field of view. This can be used to detect a moving object, such as a person, in dimly lit areas.

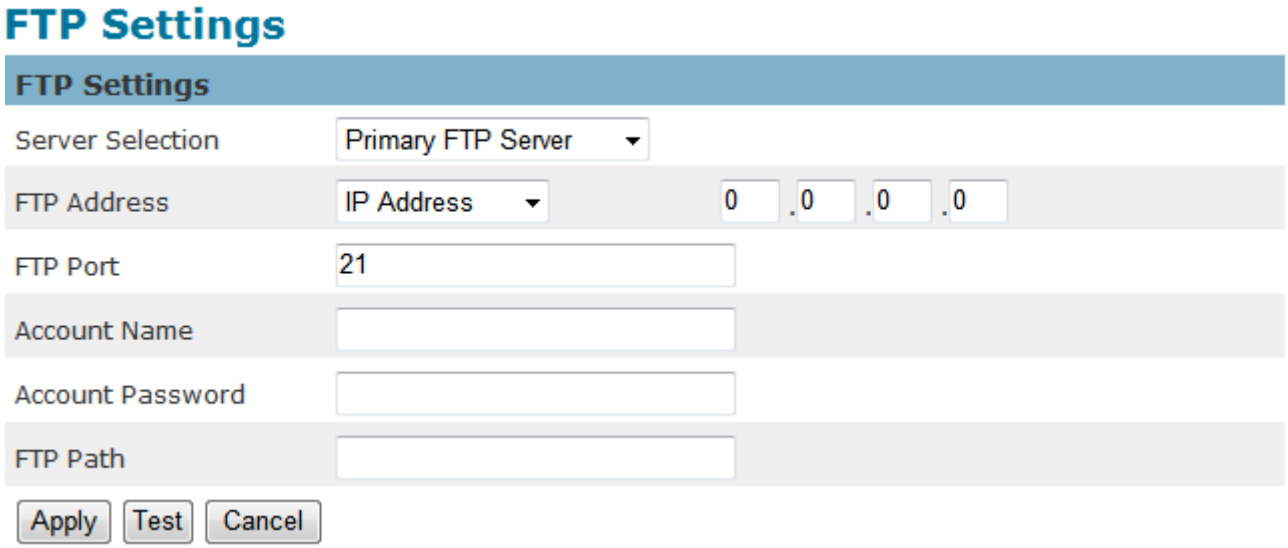
Sensitivity – Adjust the sensitivity of the PIR Sensor from the drop down menu. The sensitivity can be set from 10 - 100%; with the default sensitivity set at 50%. Higher sensitivity levels will increase the range of the PIR Sensor. When the sensitivity level is set to 100%, the PIR sensor will be able to detect moving objects within six meters.

Notifications

Use the tools in this section to specify what type of notification will be sent when an event occurs. The camera can send buffered images to an FTP server, Samba, Email, or HTTP.

FTP Settings

File Transfer Protocol (FTP) is used as an application component to automatically transfer files for program internal functions. Select “Primary FTP Server” from the Server Selection drop down menu to send media files to a FTP server when an event is triggered. Enter the FTP IP address or hostname. By default, the FTP port server is set to 21. Enter the account name, password and FTP Path to configure the settings.



Click **Apply** to apply settings or **Cancel** to cancel changes.

E-mail Settings

Select “Primary Email Server” option from the Server Selection drop down menu to send media files to an email server when an event is triggered.

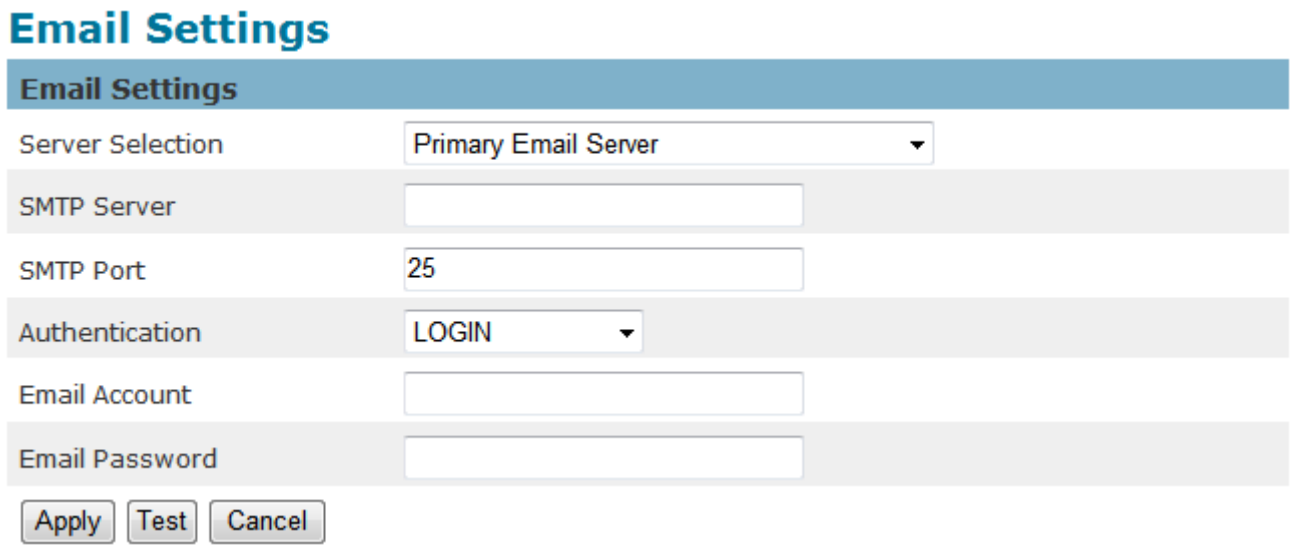
SMTP Server - Enter the server host name of the email server.

SMTP Port - Enter the port number of the email server; by default, the SMTP port is set to 25.

Authentication - Select the authentication type from the drop-down menu.

Email Account - Enter the user name of the email account if necessary.

Email Password - Enter the password of the email account if necessary.



Click **Apply** to apply settings or **Cancel** to cancel changes.

Samba Settings

Select this option to send the media files via a network neighborhood when an event is triggered.

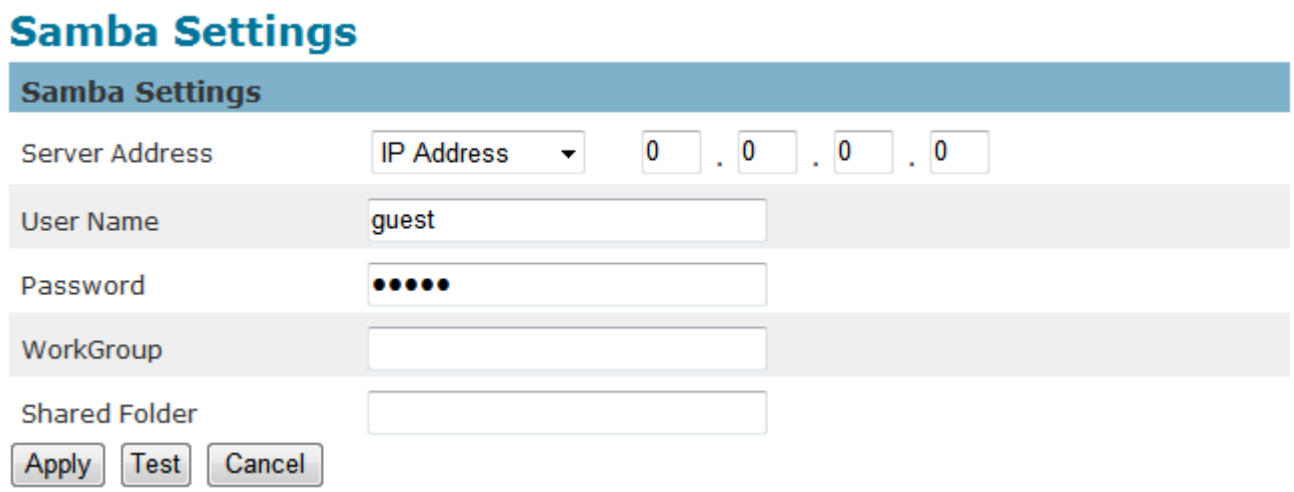
Server Address - Enter the IP address of the Samba server.

User Name - Enter the user name of the Samba server.

Password - Enter the password of the Samba server.

Work Group - Enter the workgroup of the Samba server.

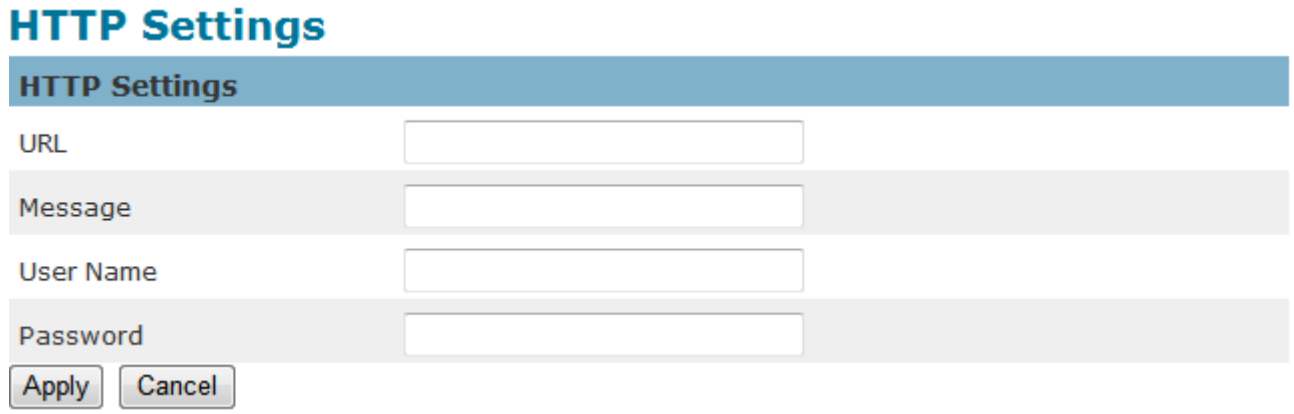
Shared Folder - Enter the share folder of the Samba server.



Click **Apply** to apply settings or **Cancel** to cancel changes.

HTTP Settings

Select this option to send the media files via an HTTP notification when an event is triggered.



URL –Specify the URL to send HTTP requests. The URL is normally written as:

http://ip_address/ notification.cgi?parameter

ip_address – type the IP address or host name of the HTTP host.

Parameter – type the notification parameter if necessary.

Example

URL - http://192.168.1.1/xxxx.cgi

Message - name1=value1&name2=vlaue2

Result - http://192.168.1.1/xxxx.cgi? name1=value1&name2=vlaue2

Ex:

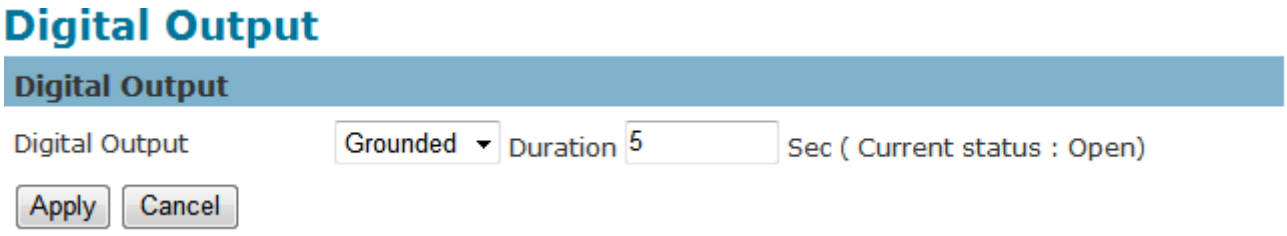
https://192.168.1.1/notification.cgi?event=MD&camera=FB-100A

Message - Enter the message notification that will be sent when an event is triggered.

Enter the user name and password if necessary.

Click **Apply** to apply settings or **Cancel** to cancel changes.

Digital Output (DO) (*)



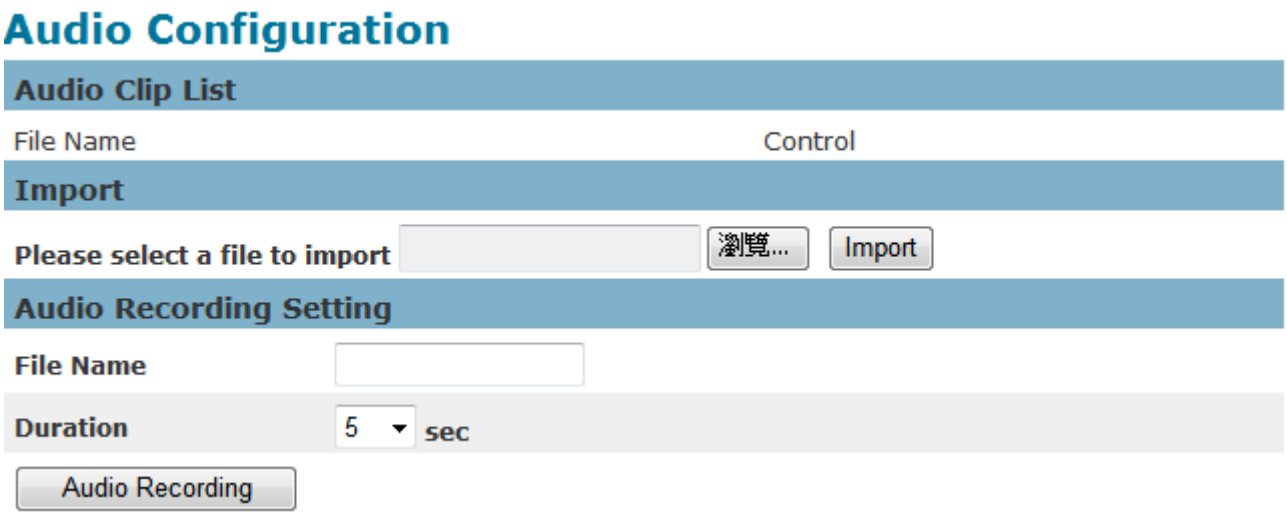
The DO socket allows the IP camera to send output to an external device. While executing the DO notification action, the IP camera drives voltage on the connected DO wire to the triggering voltage level for X number of seconds. The connected external device will then be triggered for X number of seconds.

Triggered Voltage Level - OPEN or GROUND

Users should select the option according to the specification of their external device.

Audio Clip(*)

Audio Recording – Audio clips can be recorded and played when an event occurs.

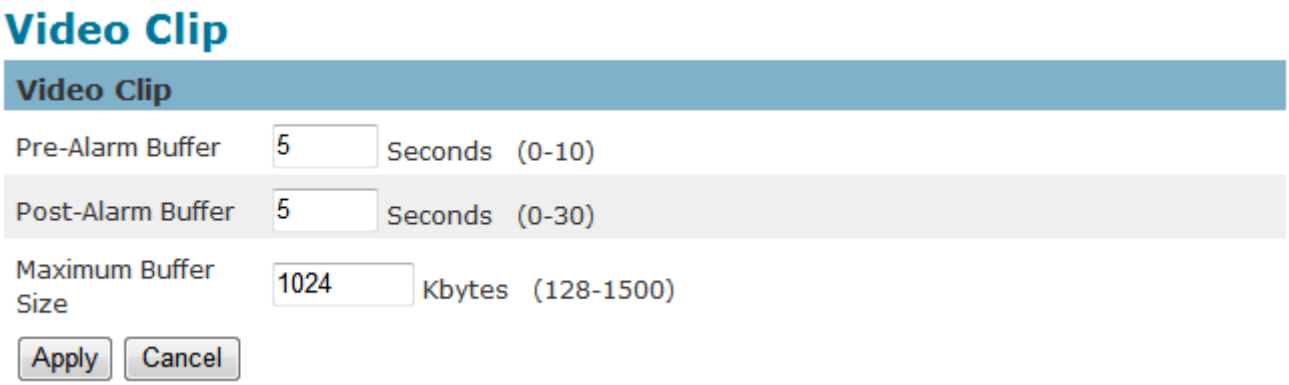


Click **Browse** to import a file from a local hard drive or network disk. Select the file and click **Import.** **NOTE** – The camera can only play audio clips which are saved as .wav files with G.711 u-law encoding in 8000 Hz sampling rate.

To record a new clip using the camera's microphone:

1. File Name-Enter a file name.
2. Duration - Enter the number of seconds to record.
3. Click **Record** to record the new audio clip.
4. The new audio clip will appear on the audio clip list.
5. Select an audio clip file from the Audio Clip List.
    a. Play- Select to hear the audio clip
    b. Stop- Select to stop playing the audio clip.
    c. Delete- Select to delete an audio clip.
    d. Export- Select to export the audio clip to a local hard drive or network disk.

Video Clip



Video Clip

This function is used to determine when video clips will be recorded and stored after an event is triggered.

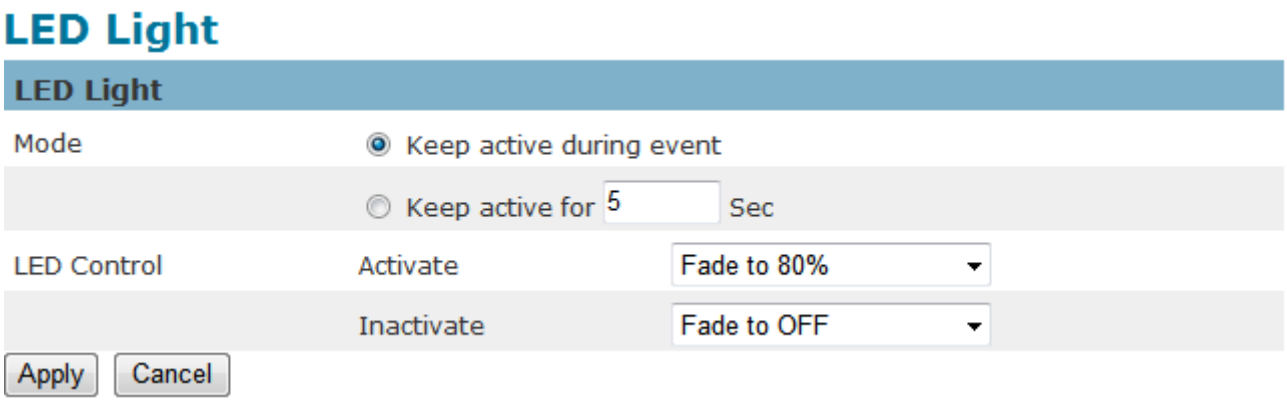
Pre-alarm buffer - Images can be stored internally on the server from the time immediately preceding the trigger. Enter the desired length of time.

Post-alarm buffer - Images can be stored internally on the server from the time immediately following the trigger. Enter the desired length of time.

Maximum buffer size –Specify the maximum file size allowed.

Click **Apply** to apply settings or **Cancel** to cancel changes.

LED Light (*)



Mode – Select “Keep active during event” or “Keep active for” a specific amount of time when an event is triggered.

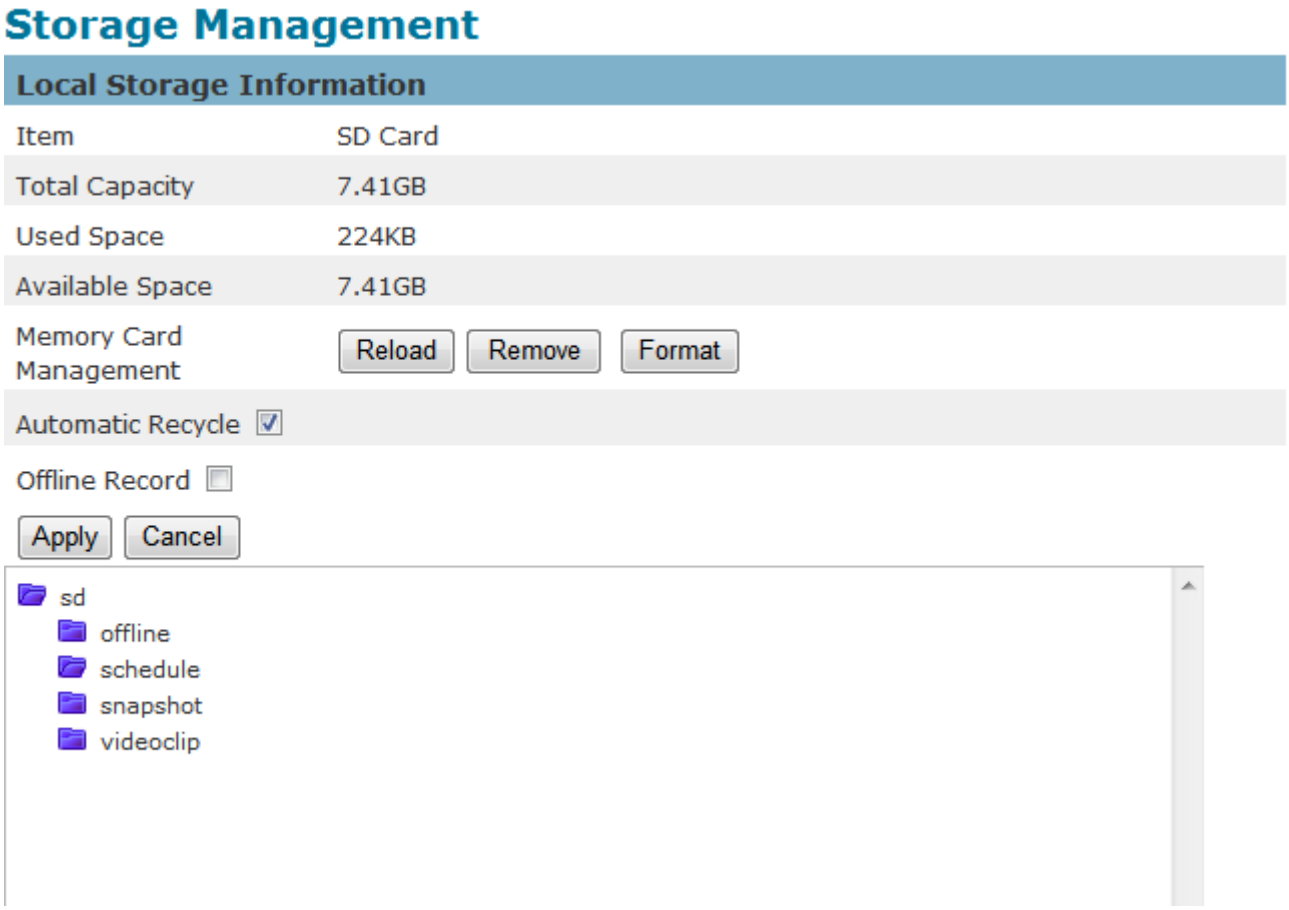
LED Control - The LED on the front of the camera can be set to flash at a configurable interval when an event is triggered. From the Activate drop down menu, select a percentage which the LED will brighten to. When the LED reaches the selected percentage, it can be configure to fade to off or turn off. Select the option from the Inactive menu.

Click **Apply** to apply settings or **Cancel** to cancel changes.

SD Card

Storage Management (*)

Storage Management is used to view all the recorded files on the Micro-SD/SDHC card.



Click **Reload** to refresh the list of recorded files.

Click **Remove** to safely remove the Micro-SD/SDHC memory card.

Click **Format** to format the Micro-SD/SDHC memory card.

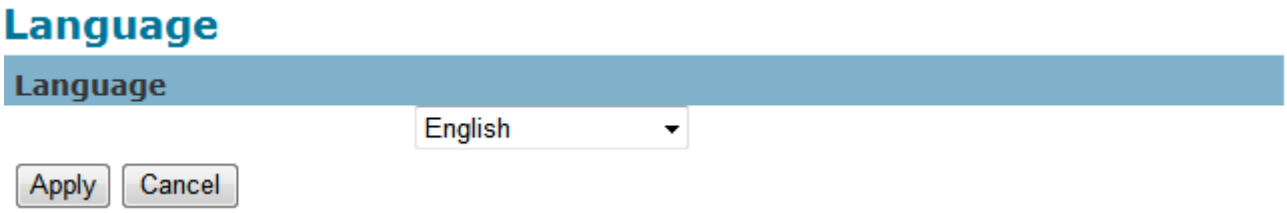
Left click on the folder to list the recorded files. The user can either play the snapshot of the recorded files by moving the mouse pointer over the file or double click on a file to play it.

Right click on the folder to download, play or delete the recorded files.

NOTE – The user may need to install QuickTime multimedia framework to play the video clips.

Maintenance

Language



Select the desired language from the drop-down list.

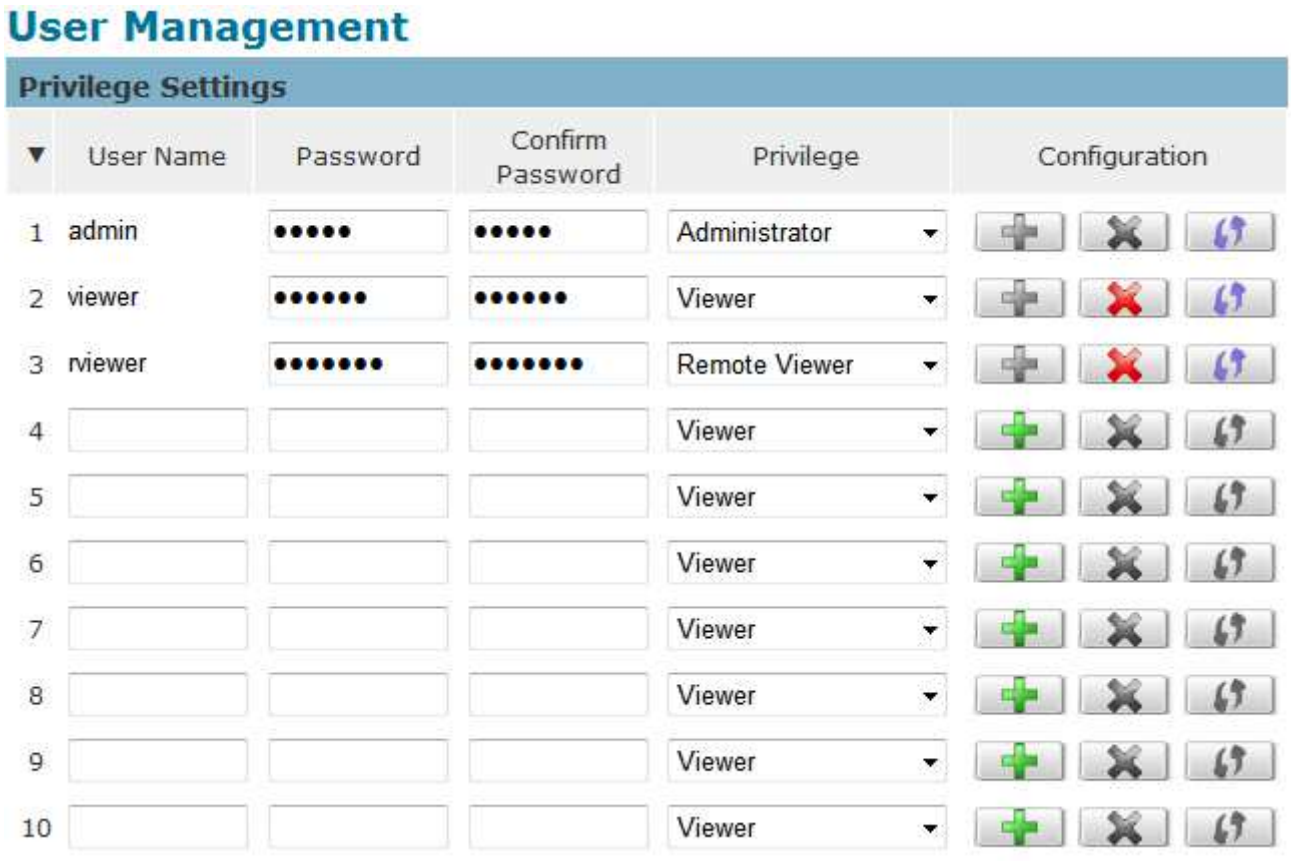
Click **Apply** to apply settings or **Cancel** to cancel changes.

User Management

This section explains how to enable password protection and create multiple accounts.

The administrator account name is “admin”, which is permanent and cannot be deleted.

Click to create an account.



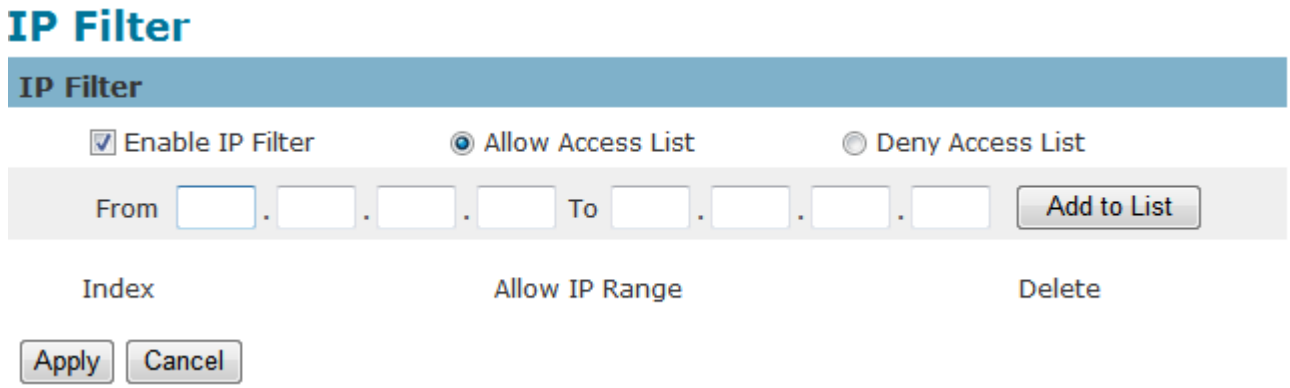
Enter the new user’s name, password and confirm password. Administrators can add up to 10 user accounts.

Select the privilege level for the new user account from the drop-down list. Privilege levels can be assigned as:

- Administrator - user has access to view and change the Configuration page. Users with administrator privilege can change other user's access rights and delete user accounts. Click **Delete** or **Update** to delete or modify a user's account.
- Viewer - user can only access the main page for live viewing.
- Remote Viewer - user can only access the main page for live viewing using TCP protocol.

IP Filter

The IP Filter is used to filter the IP addresses which are able to access the network camera. Enable the IP Filter and select to allow or deny a range of IP addresses access to the server. Click **Add to list** to add the IP range to the IP filter list.



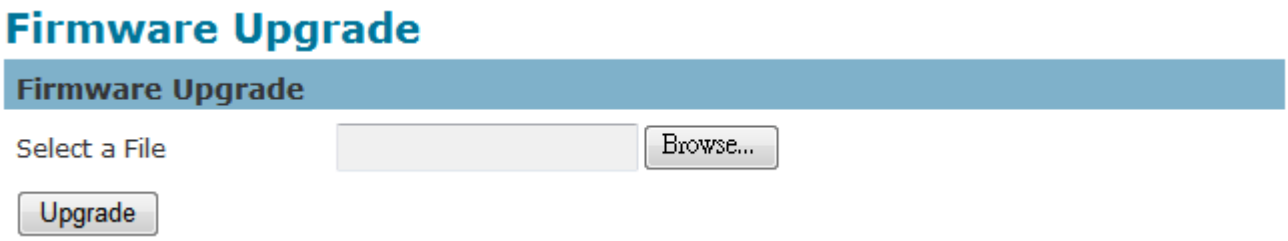
Click **Apply** to apply settings or **Cancel** to cancel changes.

Firmware Upgrade

This feature allows the user to upgrade the camera firmware. It will take a few minutes to complete the process.

NOTE - Do not power off the camera or camera during the upgrade.

Upgrade - Click **Browse…** and specify the firmware file. Click **Upgrade**. The camera will begin upgrading and will reboot automatically when the upgrade is finished.



The following message will show during the firmware upgrading process.

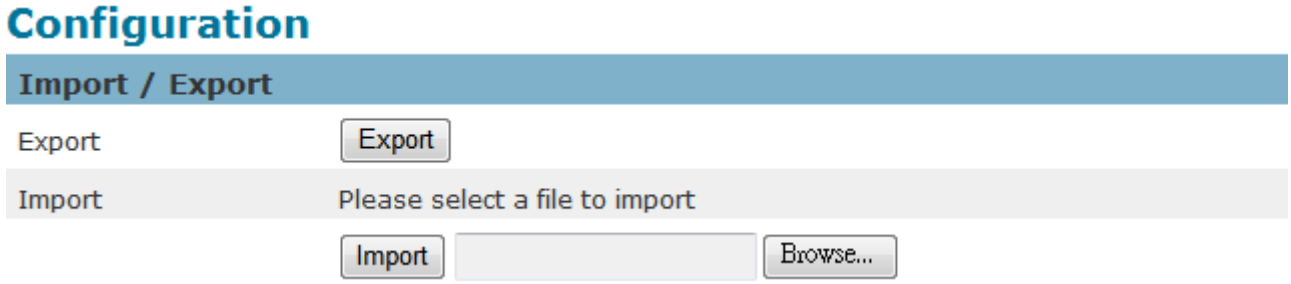
WARNING: DO NOT UNPLUG THE ETHERNET CABLE OR THE POWER CORD DURING THE FIRMWARE UPGRADE!
7%
Uploading the firmware image file...

Configuration

This feature allows the user to export/import the configuration files of the network camera.

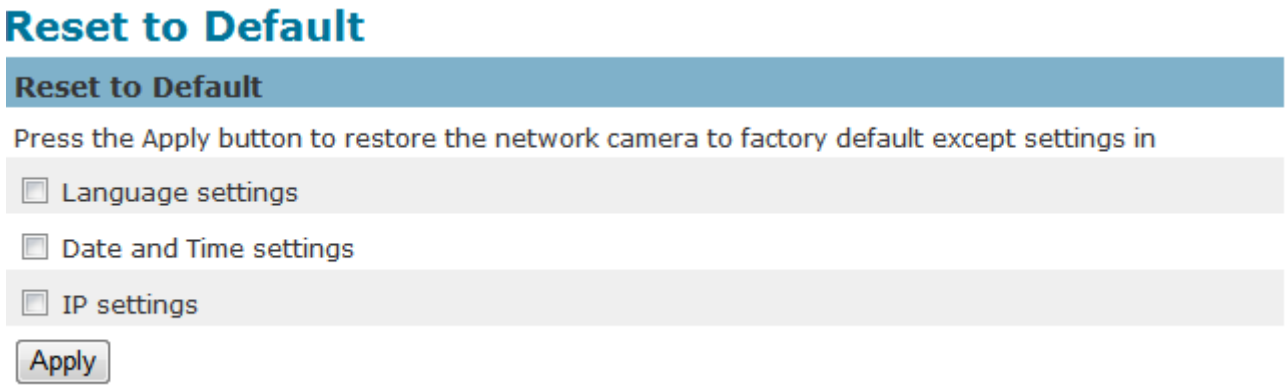
Import/Export - Click **export** to pop up a dialog to indicate the location and file to export.

Click **browse** to indicate the location and file of the camera configuration and click **import** to import the configuration file back into the network camera.



Reset to Default

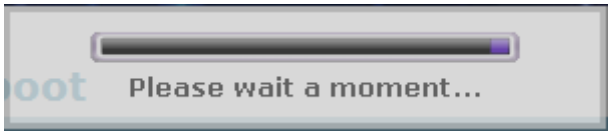
This section is used to restore the camera to default factory settings. Check the boxes to preserve the IP, Date and Time, or Language settings. Click **Apply** to restore the camera to default factory settings.


Reset to Default
Reset to Default
Press the Apply button to restore the network camera to factory default except settings in
Language settings
Date and Time settings
IP settings
Apply

Reboot

This feature will reboot the camera. Click **Apply** to begin. A message will pop up asking “The device will reboot. Are you sure?” Click “OK” to continue. The camera will take about one minute to reboot.

The following message will show during the rebooting process.

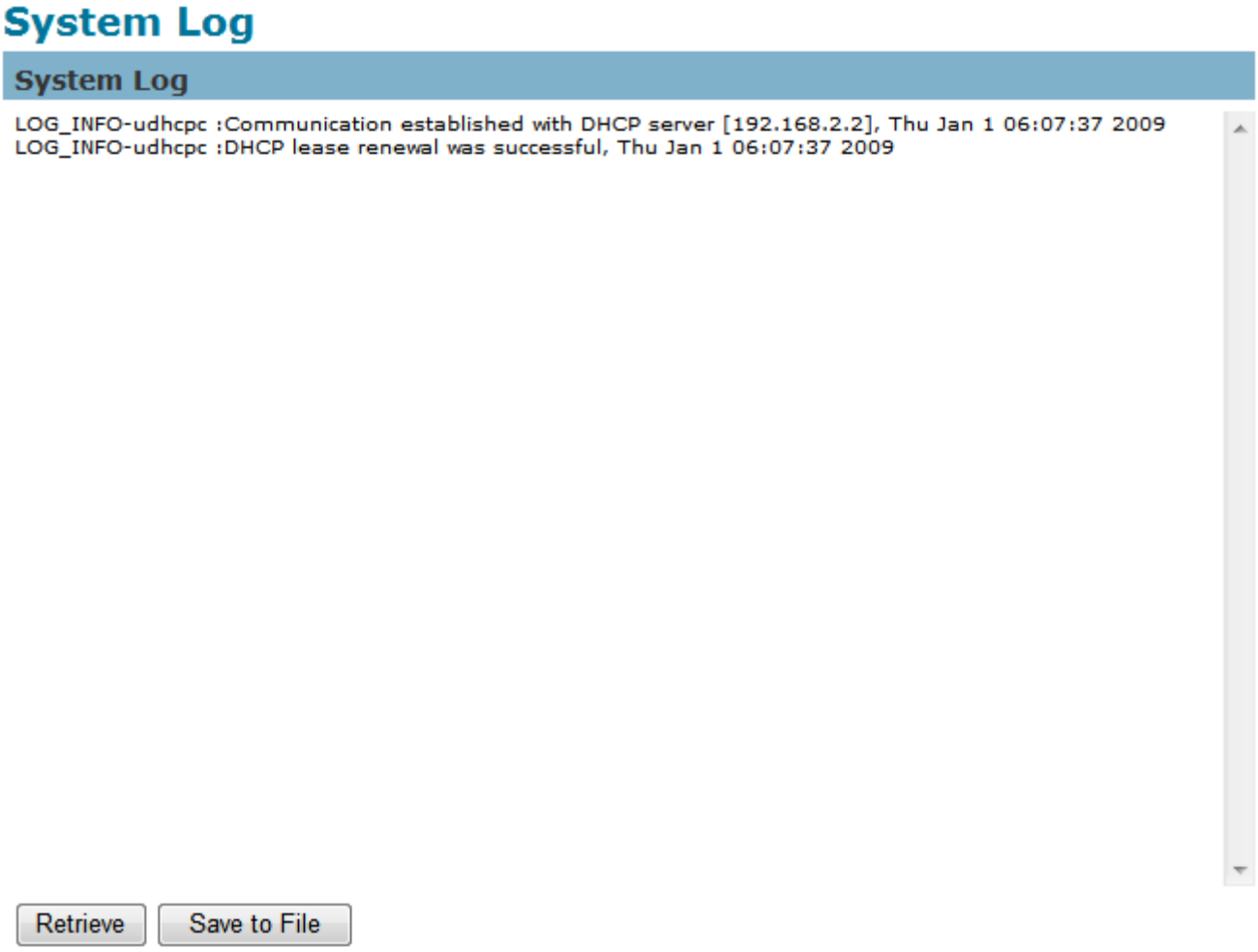


When completed, the live video page will be displayed in the web browser.

System

System Log

Log – Set up the camera to record a system log when an event is triggered.


System Log
System Log
LOG_INFO-udhcpc :Communication established with DHCP server [192.168.2.2], Thu Jan 1 06:07:37 2009
LOG_INFO-udhcpc :DHCP lease renewal was successful, Thu Jan 1 06:07:37 2009
Retrieve
Save to File

This page displays the system's log in chronological order. The system log is stored in the camera's buffer area and will be overwritten when the buffer area is full.

Click **Retrieve** to retrieve the log or click **Save to file** to save the system log.

Date and Time

Time Zone – Select the local time zone from drop-down menu.

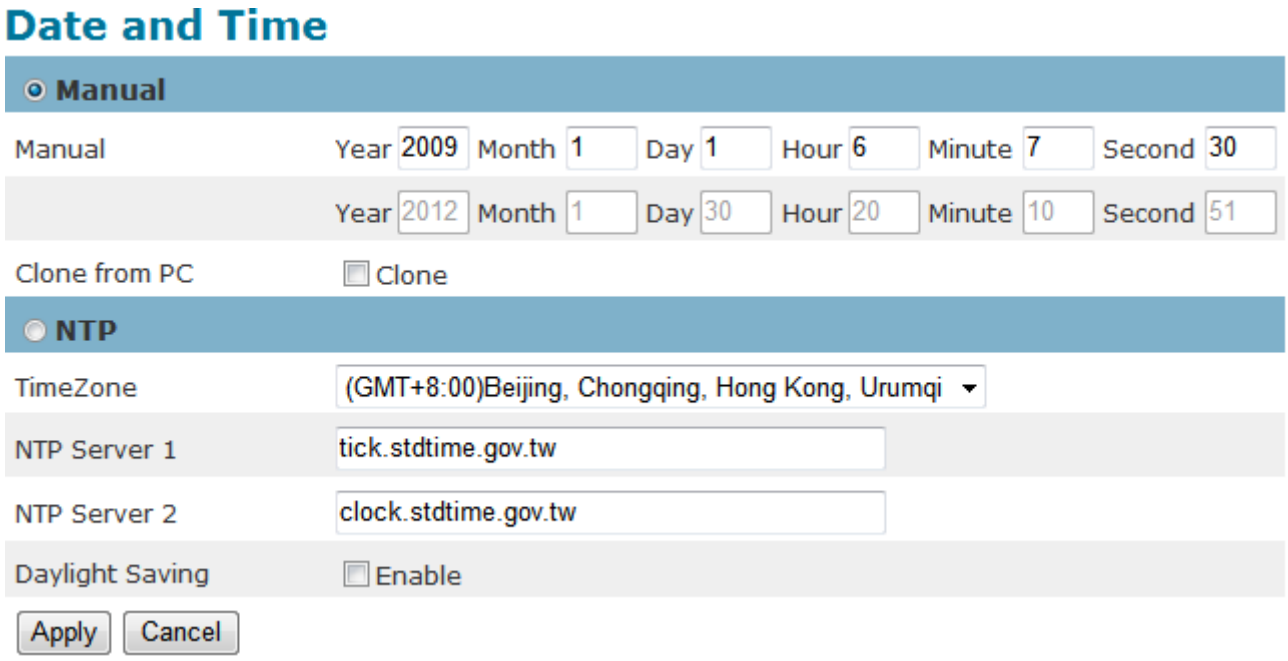
Manual – Manually enter the date and time.

Clone from PC – The camera will sync with the time, date and time zone of the computer used to modify the camera settings. Check “Clone” to utilize this option. The read-only date and time of the PC will be displayed.

NTP – (Network Time Protocol) - NTP is a protocol for synchronizing the clocks of a computer system. Select to update the time with a NTP server on an hourly, daily, weekly, or monthly basis.

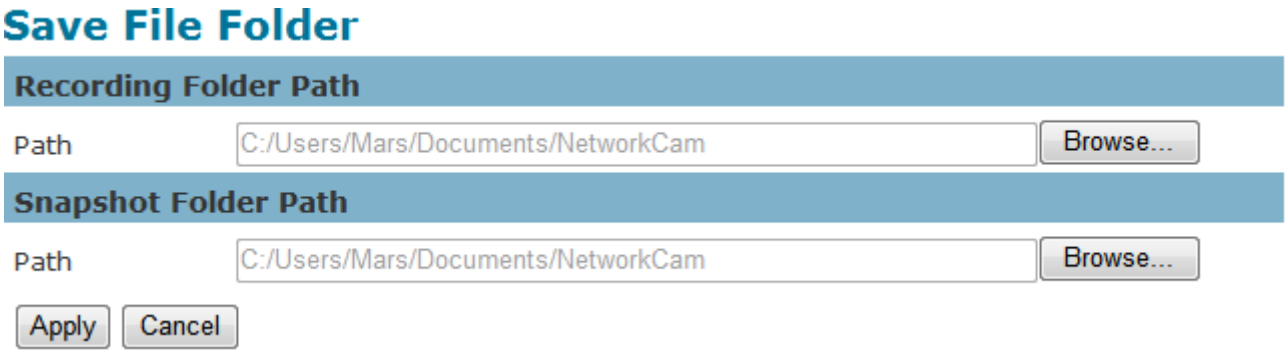
NTP Server 1 and Server 2 - Enter the address of the NTP server

Daylight Saving - Enable this option to automatically update for Daylight Savings Time.



Click **Apply** to apply settings or **Cancel** to cancel changes.

Save File Folder



Recording folder path - The destination for saving the recording video files. Click Browse to specify the saving path.

Snapshot folder path - The destination for saving the snapshot files. Click Browse to specify the saving path and select the format from the drop-down menu.

Device Information

System Information – Displays the complete system information of the camera.

Device Information

System Information	
LAN MAC Address	00:11:6b:70:fe:69
Firmware Version	v1.0.3.7
Firmware Release Date	12/28/2011 21:21
UPnP Name	C1100-fe69
Network Settings	
IP Setting Type	DHCP
IP Address	192.168.2.24
Subnet Mask	255.255.255.0
Default Gateway	192.168.2.2
Primary DNS	192.168.2.2
Secondary DNS	10.5.1.101
UPnP	Enable
DynDNS	Disable
TZO	Disable
Video/Audio Settings	
Stream 1	
Video Codec	H264
Video Resolution	1280x800(WXGA)
Video Frame Rate	15 fps
Video Bitrate	2000 Kbps
Audio Codec	N/A
Multicast IP	N/A
Stream 2	
Video Codec	MJPEG
Video Resolution	1280x800(WXGA)
Video Frame Rate	15 fps
Video Quality	3
Audio Codec	N/A
Multicast IP	N/A

Network Settings –Displays the complete network settings information of the camera.

Video/Audio Settings –Displays the complete video/audio settings information of the camera.